APPLICATION OF MULTIHOMOGENEOUS COVARIANTS TO THE ESSENTIAL DIMENSION OF FINITE GROUPS

ROLAND LÖTSCHER

Abstract. We investigate essential dimension of finite groups over arbitrary fields and give a systematic treatment of multihomogenization, introduced in [KLS08]. We generalize the central extension theorem of Buhler and Reichstein, [BR97, Theorem 5.3] and use multihomogenization to substitute and generalize the stack-involved part of the theorem of Karpenko and Merkurjev [KM08] about the essential dimension of p-groups. One part of this paper is devoted to the study of completely reducible faithful representations. Amongst results concerning faithful representations of minimal dimension there is a computation of the minimal number of irreducible components needed for a faithful representation.

1. Introduction

Throughout this paper we work over an arbitrary base field k. Sometimes we extend scalars to a larger base field, which will be denoted by K. All vector spaces and representations in consideration are finite dimensional over the base field. A quasi-projective variety defined over the base field will be abbreviated as a variety. Unless stated otherwise we will always assume varieties to be irreducible. We denote by G a finite group. A G-variety is then a variety with a regular algebraic G-action $G \times X \to X, x \mapsto gx$ on it.

The *essential dimension of* G was introduced by Buhler and Reichstein [BR97] in terms of *compressions*: A *compression* of a (faithful) G-variety Y is a dominant G-equivariant rational map $\varphi\colon Y \dashrightarrow X$, where X is a faithful G-variety.

Definition 1. The *essential dimension of* G is the minimal dimension of a compression $\varphi\colon \mathbb{A}(V) \dashrightarrow X$ of a faithful representation V of G.

The notion of essential dimension is related to Galois algebras, torsors, generic polynomials, cohomological invariants and other topics, see [BR97]. There is a general definition of the essential dimension of a functor from the category of field extensions of k to the category of sets, which is due to Merkurjev, see [BF03]. The essential dimension of G corresponds to the essential dimension of the Galois cohomology functor $K \mapsto H^1(K, G)$. We shall use this only in section 9.

We take the point of view from [KS07], where the *covariant dimension of* G was introduced: A *covariant* of G (over k) is a G-equivariant (k-)rational map $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$, where V and W are (linear) representations of G (over k). The covariant φ is called *faithful* if the image of the generic point of $\mathbb{A}(V)$ has trivial stabilizer. Equivalently there exists a $\bar{k}$-rational point in the image of φ with trivial stabilizer. We denote by $\dim \varphi$ the dimension of the closure of the image of φ.

The author gratefully acknowledges support from the Swiss National Science Foundation (Schweizerischer Nationalfonds).

Definition 2. The *essential dimension of* G, denoted by $\operatorname{edim}_k G$, is the minimum of $\dim \varphi$ where φ runs over all faithful covariants over k.

The *covariant dimension of* G, denoted by $\operatorname{covdim}_k G$, is the minimum of $\dim \varphi$ where φ runs only over the regular faithful covariants over k.

The second definition of essential dimension is in fact equivalent to the first definition, which follows e.g. from [Fl08, Proposition 2.5] or from (the first part of) the following lemma:

Lemma 1. *Let W be a faithful representation of G. Then for every affine unirational faithful G-variety X there exists a faithful regular G-equivariant map $\psi\colon X \to \mathbb{A}(W)$. If X contains a k-rational point $x_0 \in X(k)$ with trivial stabilizer and $w_0 \in W$ has trivial stabilizer as well, then ψ can be chosen such that $\psi(x_0) = w_0$:*

Proof. Choose $f \in k[X]$ such that $f(x_0) = 1$ and $f(gx_0) = 0$ for $g \neq e$, and define a regular G-equivariant map $\psi\colon X \to \mathbb{A}(W)$ by

$$\psi(x) = \sum_{g \in G} f(gx) g^{-1} w_0.$$

The map ψ is faithful since w_0 is in the image of ψ. This shows the second part of the lemma. If k is infinite this immediately implies the first part since in that case the k-rational points in X and $\mathbb{A}(W)$ are dense.

Now let k be a finite field and let t be transcendental over k. Since $k(t)$ is infinite we obtain a faithful regular $k(t)$-rational G-equivariant map $X_{k(t)} \to \mathbb{A}(W \otimes k(t))$ where $X_{k(t)} = X \times_{\operatorname{Spec} k} \operatorname{Spec} k(t)$ is X with scalars extended to $k(t)$. This corresponds to a homomorphism $W^* \otimes k(t) \to k[X] \otimes k(t)$ of representations of G with faithful image, where W^* is the dual of W and $k[X]$ is the affine coordinate ring of X. Actually we may replace $k[X] \otimes k(t)$ by $U \otimes k(t)$ for some finite-dimensional sub-representation $U \subset k[X]$. By the following Lemma 2 there exists a homomorphism $W^* \to k[X]$ with faithful image, hence a faithful regular G-equivariant map $\psi\colon X \to \mathbb{A}(W)$. □ □

Lemma 2. *Let W and V be (finite-dimensional) representations of G over k. Then:*

- *If $V \otimes k(t)$ is a quotient of $W \otimes k(t)$ then W is a quotient of V.*
- *If $W \otimes k(t)$ injects into $V \otimes k(t)$ then W injects into V.*
- *If $W \otimes k(t) \to V \otimes k(t)$ is a homomorphism with faithful image, then there exists a homomorphism $W \to V$ with faithful image as well.*

Proof. To show the first claim let $\pi\colon W \otimes k(t) \twoheadrightarrow V \otimes k(t)$ denote the quotient map. Since t is transcendental over k the kernel of π can be lifted to a representation U of G over k, i.e. $\ker \pi \simeq U \otimes k(t)$. Hence

$$(W/U) \otimes k(t) \simeq (W \otimes k(t))/(U \otimes k(t)) \simeq V \otimes k(t).$$

By the theorem of Noether-Deuring this implies $W/U \simeq V$, showing the claim. The second claim follows from the first two applied to $V \otimes k(t) \twoheadrightarrow X \otimes k(t)$ and $X \otimes k(t) \hookrightarrow V \otimes k(t)$ where X is a lift of the image of $W \otimes k(t) \to V \otimes k(t)$ to a (faithful) representation of G over k. □ □

We call a faithful regular (resp. rational) covariant *minimal* if $\dim \varphi = \operatorname{covdim}_k G$ (resp. $\dim \varphi = \operatorname{edim}_k G$). For any faithful representations V and W of G there exists a minimal faithful regular (resp. rational) covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$. This

is basically another consequence of Lemma 1. At least it shows immediately that the choice of W is arbitrary and if k is infinite one can use k-rational points with trivial stabilizer as in [KS07, Proposition 2.1] to show that V can be arbitrarily chosen. For arbitrary fields use e.g. [BF03, Corollary 3.16] to see independence of the choice of V.

In sections 2 and 3 we develop the technique of multihomogenization of covariants and derive some of its basic properties. Given G-stable gradings $V = \bigoplus_{i=1}^{m} V_i$ and $W = \bigoplus_{j=1}^{n} W_j$ a covariant $\varphi = (\varphi_1, \ldots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is called multihomogeneous if the identities

$$\varphi_j(v_1, \ldots, v_{i-1}, sv_i, v_{i+1}, \ldots, v_m) = s^{m_{ij}} \varphi_j(v_1, \ldots, v_m)$$

hold true. Here s is an indeterminate and the m_{ij} are integers, forming some matrix $M_\varphi \in \mathcal{M}_{m\times n}(\mathbb{Z})$. Thus multihomogeneous covariants generalize homogeneous covariants. A whole matrix of integers takes the role of a single integer, the degree of a homogeneous covariant. It will be shown that the degree matrix M_φ and especially its rank have a deeper meaning with regards to the essential dimension of G. Theorem 12 states that if each V_i and W_j is irreducible then the rank of the matrix M is bounded from bellow by the rank of a certain central subgroup $Z(G, k)$ (the k-center, see Definition 5). Moreover if the rank of M_φ exceeds the rank of $Z(G, k)$ by $\Delta \in \mathbb{N}$ then $\operatorname{edim}_k G \leq \dim \varphi - \Delta$. This observation shall be useful in proving (partly new) lower bounds to $\operatorname{edim}_k G$ and for most applications in the sequel.

In section 4 we study faithful representations of G, especially faithful representations of small dimension. It is the representation theoretic counterpart to the results on essential dimension obtained in later sections.

Section 5 relates essential dimension and covariant dimension. It is well known that the two differ at most by 1, see the proof of [Re04], which works for arbitrary fields. By generalizing [KLS08, Theorem 3.1] (where k is algebraically closed of characteristic 0) to arbitrary fields we obtain the precise relation of covariant and essential dimension in case that G has a completely reducible faithful representation. Namely Theorem 34 says that $\operatorname{covdim}_k G = \operatorname{edim}_k G$ if and only if G (is trivial or) has a nontrivial k-center, otherwise $\operatorname{covdim}_k G = \operatorname{edim}_k G + 1$.

A generalization of a result from [BR97] is obtained in section 6 where the following situation is investigated: G is a (finite) group and H a central cyclic subgroup which intersects the commutator subgroup of G trivially. Buhler and Reichstein deduced the relation

$$\operatorname{edim}_k G = \operatorname{edim}_k G/H + 1$$

(over a field k of characteristic 0) for the case that H is a maximal cyclic subgroup of the k-center $Z(G, k)$ and has prime order p and that there exists a character of G which is faithful on H, see [BR97, Theorem 5.3]. The above theorem was generalized to arbitrary fields in [Ka06, Theorem 4.5], where for the case of $p = \operatorname{char} k > 0$ the additional assumption is made that G contains no non-trivial normal p-subgroup. Some other partial results were obtained by Brosnan, Reichstein and Vistoli in [BRV07] and [BRV08] and by Kraft and Schwarz and the author in [KLS08]. In this paper we give a complete generalization which reads like

$$\operatorname{edim}_k G = \operatorname{edim}_k G/H + \operatorname{rk} Z(G, k) - \operatorname{rk} Z(G, k)/H,$$

where we only assume that G has no non-trivial normal p-subgroups if $\operatorname{char} k = p > 0$ and that k contains a primitive root of unity of high enough order. For details see Theorem 35.

Section 7 contains two additional results about subgroups and direct products, both obtained easily with the use of multihomogeneous covariants.

In section 8 we shall use multihomogeneous covariants to generalize Florence's twisting construction from [Fl08]. The generalized technique gives a substitution for the use of algebraic stacks in the proof of the theorem of Karpenko and Merkurjev about the essential dimension of p-groups, which says that the essential dimension of a p-group G equals the least dimension of a faithful representation of G, provided that the base field contains a primitive p-th root of unity. Actually the twisting construction gives more than that. It yields a conjectural formula for the essential dimension of any group G whose socle is central (i.e. such that every nontrivial normal subgroup of G intersects the center of G nontrivially) and whose degrees of irreducible representations satisfy some divisibility property. See Corollary of Conjecture 48 for details.

In section 9 we consider the situation when multihomogenization fails. This is the case when G does not admit a faithful completely reducible representation. That can only happen if $\operatorname{char} k = p > 0$ and G contains a nontrivial normal elementary abelian p-subgroup A. Proposition 49 relates the essential dimension of G and G/A by $\operatorname{edim}_k G/A \le \operatorname{edim}_k G \le \operatorname{edim}_k G/A + 1$ when A is central.

2. The technique of multihomogenization

2.1. **Multihomogeneous maps and multihomogenization.** Most of this section can already been found in [KLS08], where multihomogenization has originally been introduced for regular covariants (over $\mathbb{C}$). We give a more direct and general approach here.

Denote by $X = \operatorname{Hom}(\cdot, \mathbb{G}_m)$ the contravariant functor from the category of commutative algebraic groups (over k) to the category of abelian groups, which takes a commutative algebraic group Γ to $X(\Gamma) = \operatorname{Hom}(\Gamma, \mathbb{G}_m)$. For example $X(T) = \mathbb{Z}^r$ if $T = \mathbb{G}_m^r$ is a split torus of rank $r = \dim T$. In particular $X(\mathbb{G}_m) = \mathbb{Z}$.

Let $T = \mathbb{G}_m^m$ and $T' = \mathbb{G}_m^n$ be split tori. Any homomorphism $D \in \operatorname{Hom}(T, T')$ corresponds to a linear map $X(D)\colon X(T') \to X(T)$ and to a matrix $M_D \in \mathcal{M}_{m\times n}(\mathbb{Z})$ under the canonical isomorphisms

$$\operatorname{Hom}(T, T') \cong \operatorname{Hom}(X(T'), X(T)) = \operatorname{Hom}(\mathbb{Z}^n, \mathbb{Z}^m) \cong \mathcal{M}_{m\times n}(\mathbb{Z})$$

In terms of the matrix $M_D =: (m_{ij})_{1\le i\le m, 1\le j\le n}$ the homomorphism D is then given by

$$D(t_1, \dots, t_n) = (t'_1, \dots, t'_m) \text{ where } t'_j = \prod_{i=1}^{n} t_i^{m_{ij}}.$$

The above isomorphisms are compatible with composition of homomorphisms $D \in \operatorname{Hom}(T, T'), D' \in \operatorname{Hom}(T', T'')$ on the left side and multiplication of matrices $M \in \mathcal{M}_{m\times n}(\mathbb{Z})$, $M' \in \mathcal{M}_{n,r}(\mathbb{Z})$ on the right side, where T'' is another split torus and $r = \operatorname{rk} T''$. That means that $M_{D'\circ D} = M_D \cdot M_{D'}$.

Let V be a vector space equipped with a decomposition $V = \bigoplus_{i=1}^m V_i$. We call V a graded vector space and associate to V the torus $T_V \subseteq \operatorname{GL}(V)$ consisting of those linear automorphisms which are a (non-zero) multiple of the identity on each

V_i. We identify T_V with $\mathbb{G}_m^m$ acting on $\mathbb{A}(V)$ by

$$(t_1, \dots, t_m)(v_1, \dots, v_m) = (t_1 v_1, \dots, t_m v_m).$$

Let $W = \bigoplus_{j=1}^n W_j$ be another graded vector space and $T_W \subseteq \mathrm{GL}(W)$ its associated torus. Let $D \in \mathrm{Hom}(T_V, T_W)$. A rational map $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is called *D-multihomogeneous* if the diagram

$$\begin{array}{ccc} T_V \times \mathbb{A}(V) & \xrightarrow{(t,v)\mapsto tv} & \mathbb{A}(V) \\ \downarrow{\scriptstyle D\times\varphi} & & \downarrow{\scriptstyle \varphi} \\ T_W \times \mathbb{A}(W) & \xrightarrow{(t',w)\mapsto t'w} & \mathbb{A}(W) \end{array} \tag{1}$$

commutes. The map φ is called *multihomogeneous* if it is D-multihomogeneous for some $D \in \mathrm{Hom}(T_V, T_W)$. In terms of the matrix $M_D =: (m_{ij})_{1\le i\le m, 1\le j\le n}$ this means:

$$\varphi_j(v_1, \dots, sv_i, \dots, v_m) = s^{m_{ij}} \varphi_j(v_1, \dots, v_m), \tag{2}$$

for all i and j, as announced in the introduction.

Example 1. Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. If $h_{ij} \in k(V_i)^*$ for $1 \le i, j \le m$ are homogeneous rational functions of degree $r_{ij} \in \mathbb{Z}$ then the map

$$\psi_h\colon \mathbb{A}(V) \to \mathbb{A}(V), \quad v \mapsto (h_{11}(v_1) \dots h_{m1}(v_m)v_1, \dots, h_{1m}(v_1) \dots h_{mm}(v_m)v_m)$$

is multihomogeneous with degree matrix equal to $M_D = (r_{ij} + \delta_{ij})_{1\le i,j\le m}$.

Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a multihomogeneous rational map. If the projections φ_j of φ to $\mathbb{A}(W_j)$ are non-zero for all j, then the homomorphism $D \in \mathrm{Hom}(T_V, T_W)$ is uniquely determined by condition (1). We shall write D_φ, X_φ and M_φ for D, $X(D)$ and M_D, respectively. If $\varphi_j = 0$ for some j then the matrix entries m_{ij} of M_φ can be chosen arbitrary. Fixing the choice $m_{ij} = 0$ for such j makes M_φ with the property (2) and the corresponding D_φ with the property (1) unique again. This convention that we shall use in the sequel has the advantage that adding or removing of some zero-components of the map φ does not change the rank of the matrix M_φ.

Given an arbitrary rational map $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ we will produce a multihomogeneous map $H_\lambda(\varphi)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ which depends only on φ and the choice of a suitable one-parameter subgroup $\lambda \in \mathrm{Hom}(\mathbb{G}_m, T_V)$. In section 3 this procedure will be applied to covariants for a group G.

Let $\nu\colon k(V \times k) = k(s)(V) \to \mathbb{Z} \cup \{\infty\}$ be the discrete valuation belonging to the hyperplane $\mathbb{A}(V) \times \{0\} \subset \mathbb{A}(V) \times \mathbb{A}^1$. So $\nu(0) = \infty$ and for $f \in k(V \times k) \setminus \{0\}$ the value of $\nu(f)$ is the exponent in which the coordinate s appears in a primary decomposition of f. Let $O_s \subset k(V \times k)$ denote the valuation ring corresponding to ν. Every $f \in O_s$ can be written as $f = \frac{p}{q}$ with polynomials p, q where $s \nmid q$. For such f we define $\lim f \in k(V)$ by $(\lim f)(v) = \frac{p(v,0)}{q(v,0)}$ on the dense open subset in $\mathbb{A}(V)$ where $q(v, 0) \neq 0$. It is non-zero if and only if $\nu(f) = 0$. Moreover $\nu(f - \lim f) > 0$ where $\lim f \in k(V)$ is considered as element of $k(V \times k)$. This follows from writing $(f - \lim(f))(v, s)$ as

$$\frac{p(v,s)}{q(v,s)} - \frac{p(v,0)}{q(v,0)} = \frac{p(v,s)q(v,0) - q(v,s)p(v,0)}{q(v,s)q(v,0)},$$

noting that s does not divide the denominator, but s divides the numerator since the numerator vanishes on the hyperplane $\mathbb{A}(V)\times\{0\}\subset\mathbb{A}(V)\times\mathbb{A}^1$. This construction can easily be generalized for rational maps $\psi\colon \mathbb{A}(V)\times\mathbb{A}^1 \dashrightarrow \mathbb{A}(W)$ by choosing coordinates on W. So for $\psi=(f_1,\dots,f_d)$ where $d=\dim W$ and $f_1,\dots,f_d\in O_s$ we shall write $\lim\psi$ for the rational map $(\lim f_1,\dots,\lim f_d)\colon \mathbb{A}(V)\dashrightarrow\mathbb{A}(W)$. One may check that this definition does not depend on the choice of the basis of W.

Let $\lambda\in\operatorname{Hom}(\mathbb{G}_m,T_V)$ be a one-parameter subgroup of T_V. Consider

$$\tilde\varphi\colon \mathbb{A}(V)\times\mathbb{G}_m \dashrightarrow \mathbb{A}(W),\quad (v,s)\mapsto\varphi(\lambda(s)v)$$

as a rational map on $\mathbb{A}(V)\times\mathbb{A}^1$. For $j=1\dots m$ let α_j be the smallest integer d such that all coordinates functions in $s^d\tilde\varphi_j$ are elements of O_s. Actually that works only if $\tilde\varphi_j\neq 0$. Otherwise we choose $\alpha_j=0$. Let $\lambda'\in\operatorname{Hom}(\mathbb{G}_m,T_W)$ be the one-parameter subgroup corresponding to α, i.e. $\lambda'(s)=(s^{\alpha_1},\dots,s^{\alpha_n})\in T_W$ for $s\in\mathbb{G}_m$. Then for $\lambda'(s)\tilde\varphi(v,s)=\lambda'(s)\varphi(\lambda(s)v)$ considered as a rational map $\mathbb{A}(V)\times\mathbb{A}^1\dashrightarrow\mathbb{A}(W)$ we can take its limit:

$$H_\lambda(\varphi)=\lim\ \big((v,s)\mapsto\lambda'(s)\varphi(\lambda(s)v)\big)\colon\mathbb{A}(V)\dashrightarrow\mathbb{A}(W).$$

The limit $H_\lambda(\varphi)=(H_\lambda(\varphi)_1,\dots,H_\lambda(\varphi)_n)$ depends only on φ and the choice of λ. By construction we have for $j=1\dots n$: $(H_\lambda(\varphi))_j\neq 0$ if and only if $\varphi_j\neq 0$.

It is quite immediate that $H_\lambda(\varphi)$ is equivariant with respect to the homomorphism of tori $\lambda(\mathbb{G}_m)\to\lambda'(\mathbb{G}_m)$ which sends $\lambda(s)$ to $\lambda'(s^{-1})$. However, to get equivariance for the full tori T_V and T_W we have to choose the one-parameter subgroup λ carefully. In any case we have the following

Lemma 3. *For any one-parameter subgroup $\lambda\in\operatorname{Hom}(\mathbb{G}_m,T_V)$ we have*

$$\dim H_\lambda(\varphi)\le\dim\varphi.$$

Proof. Choose a basis in each W_j and take their union for a basis of W. Let $d=\dim W$ and write $\varphi=(f_1,\dots,f_d)$ with respect to the chosen basis, where $f_j\in k(V)$. Then $H_\lambda(\varphi)$ is of the form $(\lim\hat f_1,\dots,\lim\hat f_d)$ where each $\hat f_j\in O_s\subset k(V\times k)$ is given by

$$\hat f_j(v,s)=s^{\gamma_j}f(\lambda(s)v)$$

for some $\gamma_j\in\mathbb{Z}$. Choose a maximal subset $S=\{j_1,\dots,j_l\}$ of $\{1,\dots,d\}$ with the property that $\lim\hat f_{j_1},\dots,\lim\hat f_{j_l}$ are algebraically independent. It suffices to show that $f_{j_1},\dots,f_{j_l}$ are then algebraically independent, too. Without loss of generality $j_1=1,\dots,j_l=l$.

Assume that $f_1,\dots,f_l$ are algebraically dependent. Let $p\in k[x_1,\dots,x_l]\setminus\{0\}$ with $p(f_1,\dots,f_l)=0$. Since the algebraic independence implies $\lim\hat f_j\neq 0$ for $j=1\dots l$ we have $\nu(\hat f_j)=0$. Set $\gamma=(\gamma_1,\dots,\gamma_l)$ and write p in the form

$$p=\sum_{i\in\mathbb{Z}}p_i\quad\text{where}\quad p_i=\sum_{\beta\in\mathbb{N}^l\colon\,\beta\cdot\gamma=-i}c_\beta x_1^{\beta_1}\cdots x_l^{\beta_l}.$$

Let $d=\min\{i\in\mathbb{Z}\mid\exists\beta\in\mathbb{N}^l\colon\beta\cdot\gamma=-i,c_\beta\neq 0\}$. That implies $p_d\neq 0$. For $j=1\dots l$ there exists $\delta_j\in O_s\subset k(V\times k)$ such that $\hat f_j-\lim\hat f_j=s\delta_j$. By construction,

$$\begin{aligned}0&=s^{-d}p(f_1,\dots,f_l)(\lambda(s)v)=s^{-d}p(s^{-\gamma_1}\hat f_1,\dots,s^{-\gamma_l}\hat f_l)(v)\\&=s^{-d}p\big(s^{-\gamma_1}(\lim\hat f_1+s\delta_1),\dots,s^{-\gamma_l}(\lim\hat f_l+s\delta_l)\big)(v)\\&=p_d\big(\lim\hat f_1,\dots,\lim\hat f_l\big)(v)+sh(v,s),\end{aligned}$$

where $h \in O_s$. Taking the limit shows $p_d\big(\lim \hat{f}_1, \dots, \lim \hat{f}_l\big) = 0$, which concludes the proof. □ □

Now the goal is to find a one-parameter subgroup $\lambda \in \mathrm{Hom}(\mathbb{G}_m, T_V)$ such that $H_\lambda(\varphi)$ becomes multihomogeneous. We can assume that $\varphi_j \neq 0$ for all j. Write φ in the form $\varphi = \frac{1}{f}(\psi_1, \dots, \psi_n)$ where each $\psi_j \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W_j)$ is regular and $f \in k[V]$. The space $\mathrm{Mor}(V, W_j)$ of regular maps $\mathbb{A}(V) \to \mathbb{A}(W_j)$ carries a representation of T_V where W_j is equipped with the trivial action of T_V. It decomposes into a direct sum $\mathrm{Mor}(V, W_j) = \bigoplus \mathrm{Mor}(V, W_j)_\chi$ taken over all $\chi \in X(T_V)$, where

$$\mathrm{Mor}(V, W_j)_\chi = \{\psi \in \mathrm{Mor}(V, W_j) \mid \psi(t^{-1}v) = \chi(t)\psi(v) \text{ for all } t \in T_V, v \in \mathbb{A}(V)\}.$$

Thus $\psi_1, \dots, \psi_n$ can be written as a sum $\psi_j = \sum_\chi \psi_j^\chi$ where only finitely many ψ_j^χ are different from 0. Similarly $f \in k[V] = \mathrm{Mor}(V, k)$ has a decomposition $f = \sum_\chi f^\chi$ with the same properties. Let

$$S(\psi, f) = \{\chi \in X(T_V) \mid f^\chi \neq 0 \text{ or } \exists j : \psi_j^\chi \neq 0\},$$

which is a finite subset of $X(T_V)$.

Lemma 4. *If T is a split torus and $S \subset X(T)$ is a finite subset then there exists a one-parameter subgroup $\lambda \in \mathrm{Hom}(\mathbb{G}_m, T)$ such that the restriction of the map $X(T) \to \mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m), \chi \mapsto \chi \circ \lambda$ to S is injective.*

Proof. The claim can easily be shown via induction on the rank $r = \mathrm{rk}\, T$ of the torus. Identifying $X(T) = \mathbb{Z}^r = \mathrm{Hom}(\mathbb{G}_m, T)$ and $\mathrm{Hom}(\mathbb{G}_m, \mathbb{G}_m) = \mathbb{Z}$ the above map is given by $\mathbb{Z}^r \to \mathbb{Z}, \quad \alpha \mapsto \langle \alpha, \beta \rangle := \sum_{i=1}^r \alpha_i \beta_i$, where $\beta \in \mathbb{Z}^r$ corresponds to λ. □ □

We shall write $\langle \chi, \lambda \rangle$ for the image of $\chi \circ \lambda$ in $\mathbb{Z}$, i.e. $\chi \circ \lambda(s) = s^{\langle \chi, \lambda \rangle}$ for $s \in \mathbb{G}_m$. Now let λ be as in Lemma 4 where $T = T_V$ and $S = S(\psi, f)$. Set $\psi_0 = f$. Then there are unique characters $\chi_0, \chi_1, \dots, \chi_n$ such that $\chi_j \circ \lambda$ is minimal (considered as integer) amongst all $\chi \circ \lambda$ for which $\psi_j^\chi \neq 0$, for each $j = 0 \dots n$. Then the rational map $\mathbb{A}(V) \times \mathbb{A}^1 \dashrightarrow \mathbb{A}(W_j)$ (or $\mathbb{A}(V) \times \mathbb{A}^1 \dashrightarrow \mathbb{A}^1$ for $j = 0$) given by

$$\begin{aligned} s^{-\langle \chi_j, \lambda \rangle} \psi_j(\lambda(s)v) &= s^{-\langle \chi_j, \lambda \rangle} \sum_\chi \psi_j^\chi(\lambda(s)v) \\ &= s^{-\langle \chi_j, \lambda \rangle} \sum_\chi \chi \circ \lambda(s) \psi_j^\chi(v) \\ &= \sum_\chi s^{\langle \chi - \chi_j, \lambda \rangle} \psi_j^\chi(v) \end{aligned}$$

has limit $\psi_j^{\chi_j}$, which implies that $H_\lambda(\varphi) = \frac{1}{f^{\chi_0}}(\psi_1^{\chi_1}, \dots, \psi_n^{\chi_n})$. Define the homomorphism $D \in \mathrm{Hom}(T_V, T_W)$ by

$$D = (\chi_1 \chi_0^{-1}, \dots, \chi_n \chi_0^{-1}).$$

Then $H_\lambda(\varphi)(tv) = D(t) H_\lambda(\varphi)(v)$, showing that $H_\lambda(\varphi)$ is D-multihomogeneous.

2.2. **Existence of minimal multihomogeneous covariants.** We now go over to the case where the graded vector spaces $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ are furnished with a representation of G. We assume that the tori T_V and T_W commute with the action of G on V and W, respectively. Equivalently, the subspaces V_i and W_j are G-invariant. We will then represent a covariant $\varphi \colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$

as $\varphi = \frac{1}{f}\psi$ where $\psi\colon \mathbb{A}(V) \to \mathbb{A}(W)$ is a regular covariant and $f \in k[V]^G$. For $\lambda \in \operatorname{Hom}(T_V, T_W)$ as in Lemma 4 the rational map $H_\lambda(\varphi)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is then multihomogeneous and has dimension $\dim H_\lambda(\varphi) \le \dim \varphi$. Moreover, $H_\lambda(\varphi)$ is again a covariant, since the weight spaces $\operatorname{Mor}(V, W_j)_\chi$ and $\operatorname{Mor}(V, k)_\chi$ are G-stable, so for $j = 1 \dots n$ the maps ψ_j^χ and in particular $\psi_j^{\chi_j}$ are covariants for G and the functions f^χ and in particular f^{χ_0} are invariants. In general $H_\lambda(\varphi)$ does not have to be faithful if φ is. However:

Lemma 5. *If the representations $W_1, \dots, W_n$ are all irreducible, then $H_\lambda(\varphi)$ is faithful as well.*

Proof. Let N_j and N_j' denote the stabilizer of the image of the generic point of φ_j and $H_\lambda(\varphi_j)$, respectively. It suffices to show $N_j = N_j'$ for $j = 1 \dots n$. If φ_j is zero then $H_\lambda(\varphi_j) = 0$ as well and $N_j = G = N_j'$. In the other case both maps are nonzero and their images are G-stable subsets of $W_j \otimes k(V)$ spanning $W_j \otimes k(V)$ linearly (since $W_j \otimes k(V)$ is irreducible). Thus N_j and N_j' are both equal to the kernel of the action of G on W_j. Again $N_j = N_j'$. □ □

Thus if we have a minimal faithful covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ and $W = \bigoplus_{j=1}^n W_j$ is a decomposition into irreducible sub-representations, we can always replace it by the multihomogeneous covariant $H_\lambda(\varphi)$ without loosing faithfulness or minimality.

Note that a completely reducible faithful representation W does not exist for every choice of G and k. For example if $k = \bar{k}$ and the center of G has an element g of prime-order p, then g acts as a primitive p-th root of unity on some of the irreducible components of W. That is only possible if $\operatorname{char} k \neq p$. We use the following:

Definition 3. G is called *semi-faithful* (over k) if it admits a completely reducible faithful representation (over k).

A criterion for a group to admit a completely reducible faithful representation with any fixed number of irreducible components was given by Shoda [Sh30] (in the ordinary case) and Nakayama [Na47] (in the modular case). In particular Nakayama obtained [Na47, Theorem 1] that G is semi-faithful over a field of $\operatorname{char} k = p > 0$ if and only if it has no nontrivial normal p-subgroups. One direction follows from Clifford's theorem which says that the restriction of a completely reducible representation to a normal subgroup is again completely reducible and the fact that the only irreducible representation of a p-group in characteristic p is the trivial one. For the other implication see Lemma 19. Therefore we get the following

Corollary 6. *If either $\operatorname{char} k = 0$, or $\operatorname{char} k = p > 0$ and G has no nontrivial normal p-subgroup, there exists a multihomogeneous minimal faithful covariant for G.*

2.3. **Multihomogeneous invariants.** Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. An element $f \in k(V)$ is called *multihomogeneous* if it is multihomogeneous regarded as a rational map $\mathbb{A}(V) \dashrightarrow \mathbb{A}^1$. Let G be semi-faithful and V a faithful completely reducible representation. The non-zero multihomogeneous invariants form a group under multiplication, denoted by $\mathcal{M}_G(V)$. It is a system of generators for the field $k(V)^G$ of invariants.

Definition 4. The *degree module* $\mathrm{DM}_G(V)$ of V is the submodule of $X(T_V) \simeq \mathbb{Z}^m$ formed by the degrees of multihomogeneous invariants, i.e. the image of the group homomorphism $\deg\colon \mathcal{M}_G(V) \to X(T_V), \quad f \mapsto D_f(\mathrm{Id}_{\mathbb{G}_m})$. Equivalently it is the image of the group homomorphism

$$\prod_{f\in S} X(\mathbb{G}_m) \to X(T_V)$$

induced by the homomorphisms $X(D_f)\colon X(\mathbb{G}_m) \to X(T_V)$, where $S \subseteq \mathcal{M}_G(V)$ is any finite subset whose degrees generate $\mathrm{DM}_G(V)$.

Definition 5. The central subgroup

$$Z(G,k) := \{g \in Z(G) \mid \zeta_{\operatorname{ord} g} \in k\}$$

of G is called the *k-center* of G.

The k-center of G is the largest central subgroup Z for which k contains a primitive root of unity of order $\exp Z$. The groups $Z(G,k)$ and $X(Z(G,k)) = \mathrm{Hom}(Z(G,k), \mathbb{G}_m)$ are (non-canonically) isomorphic. The elements of $Z(G,k)$ are precisely the elements of G which act as scalars on every irreducible representation of G over k:

Lemma 7. *Let $V = \bigoplus_{i=1}^m V_i$ be any completely reducible faithful representation. Then $\rho_V(Z(G,k)) = T_V \cap \rho_V(G)$.*

Proof. Since both sides are abelian groups it suffices to prove equality for their Sylow-subgroups. Let p be a prime ($p \neq \operatorname{char} k$) and $g \in Z(G)$ be an element of order p^l for some $l \in \mathbb{N}_0$. We must show that the following conditions are equivalent:

(A) g acts as a scalar on every V_i
(B) $\zeta_{p^l} \in k$.

Since V is faithful the order of g equals the order of $\rho(g) \in \mathrm{GL}(V)$, hence the first condition implies the second one. Conversely let $\rho''\colon G \to \mathrm{GL}(V_0)$ be any irreducible representation of G. Then the minimal polynomial of $\rho''(g)$ has a root in k since it divides $T^{p^l} - 1 \in k[T]$ which factors over k assuming the second condition. Hence $\rho''(g)$ is a multiple of the identity on V'. In particular this holds for $G \to \mathrm{GL}(V_i)$, proving the claim. □ □

Degree module and the k-center of G are related as follows:

Proposition 8. *The sequence $\mathcal{M}_G(V) \xrightarrow{\deg} X(T_V) \to X(Z(G,k)) \to 1$ is exact and in particular $X(T_V)/\mathrm{DM}_G(V) \cong X(Z(G,k)) \simeq Z(G,k)$.*

Proof. Choose a finite subset $S \subseteq \mathcal{M}_G(V)$ such that the degrees of S generate $\mathrm{DM}_G(V)$. We may replace the homomorphism $\deg\colon \mathcal{M}_G(V) \to X(T_V)$ by the homomorphism $X(\prod_{f\in S} \mathbb{G}_m) \to X(T_V)$, since they both have image $\mathrm{DM}_G(V)$. Now the claim becomes equivalent to exactness of the sequence

$$1 \to Z(G,k) \to T_V \to \prod_{f\in S} \mathbb{G}_m.$$

Exactness at $Z(G,k)$ follows directly from faithfulness of V. Denote by Q the kernel of the last map, which is the intersection of the kernels of the maps $D_f\colon T_V \to \mathbb{G}_m$ taken over all multihomogeneous invariants $f \in S$. Clearly $\rho_V(Z(G,k)) \subseteq Q$ because f is G-invariant. On the other hand let $\tilde{G}$ be the subgroup of $\mathrm{GL}(V)$

generated by $\rho_V(G)$ and Q. Then $\mathcal{M}_G(V) = \mathcal{M}_{\tilde{G}}(V)$ and therefore $k(V)^G = k(V)^{\rho_V(G)} = k(V)^{\tilde{G}}$. This can only happen if $\rho_V(G) = \tilde{G}$. By Lemma 7 this implies $Q = \rho_V(Z(G,k))$, showing the claim. □ □

Let $\varphi = (\varphi_1, \dots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant and let $f_1, \dots, f_n \in \mathcal{M}_G(V)$ be multihomogeneous invariants. Then $\tilde{\varphi} = (f_1\varphi_1, \dots, f_n\varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is again a faithful covariant. That induces an action of the group $\mathcal{M}_G(V)^n$ on the space $\mathrm{mCov}(V,W)$ of multihomogeneous covariants $\mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$, which respects faithfulness. Furthermore we get an action of $\mathcal{M}_G(V)^n$ on the set $S = \{X_\varphi\colon \varphi \in \mathrm{mCov}(V,W)\} \subseteq \mathrm{Hom}(X(T_W), X(T_V))$ of all degrees associated to multihomogeneous invariants. We will identify the group $\mathcal{M}_G(V)^n$ with the group $\mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$ by associating to an element $\gamma \in \mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$ the n-tuple $(f_1, \dots, f_n) \in \mathcal{M}_G(V)$ where $f_j = \gamma(\chi_j)$ for the standard basis of $X(T_W)$ formed by the characters $\chi_j\colon T_W \to \mathbb{G}_m, t = (t_1, \dots, t_n) \mapsto t_j$. Then the action on degrees is given by

$$\begin{aligned} \mathrm{Hom}(X(T_W), \mathcal{M}_G(V)) \times S &\to S, \\ (\gamma, s) &\mapsto (\gamma s\colon X(T_W) \to X(T_V) \\ \chi &\mapsto (\deg \gamma(\chi)) \cdot s(\chi). \end{aligned}$$

From Proposition 8 we get

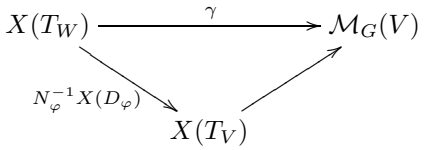
Corollary 9. *The group* $\mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$ *acts transitively on the set* S *of all degree matrices associated to multihomogeneous covariants.*

Proof. Let $s, s' \in S$ and choose $\varphi, \varphi' \in \mathrm{mCov}(V,W)$ such that $s = X_\varphi$ and $s' = X_{\varphi'}$. Define $D \in \mathrm{Hom}(T_V, T_W)$ by $D(t) = D_\varphi(t) D_{\varphi'}(t^{-1})$ for $t \in T_V$. Then $D(z) = 1$ for all $z \in \rho_V(Z(G,k))$, since D_φ and $D_{\varphi'}$ are both the identity on $\rho_V(Z(G,k))$. By Proposition 8 this is equivalent to saying that $X(D) \in \mathrm{Hom}(X(T_W), \mathrm{DM}_G(V))$. Therefore $X(D)$ comes from some homomorphism $\gamma \in \mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$. By construction $\gamma s' = s$, finishing the proof. □ □

Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant. Let $N_\varphi \in \mathbb{N}$ be the greatest common divisor of the entries of the elements of $\operatorname{im} X(D_\varphi) \subseteq X(T_V) \cong \mathbb{Z}^m$, where $m = \dim T_V$. Then $N_\varphi^{-1} X(D_\varphi)\colon X(T_W) \to X(T_V)$ is well defined and its image has a complement in $X(T_V)$. We distinct between two types of elements of $\mathrm{Hom}(X(T_W), \mathcal{M}_G(V))$ relative to φ:

Definition 6. A homomorphism $\gamma\colon X(T_W) \to \mathcal{M}_G(V)$ is called of

- *type I relative to* φ if it factors through $N_\varphi^{-1} X(D_\varphi)\colon X(T_W) \to X(T_V)$, i.e. if there exists a commutative diagram of the form



- *type II relative to* φ if the image of γ equals the image of $\ker X(D_\varphi) \hookrightarrow X(T_W) \to \mathcal{M}_G(V)$.

Proposition 10. *Every homomorphism* $\gamma\colon X(T_W) \to \mathcal{M}_G(V)$ *decomposes uniquely as* $\gamma = \alpha \cdot \beta$ *where* $\alpha\colon X(T_W) \to \mathcal{M}_G(V)$ *is of type I relative to* φ *and* $\beta\colon X(T_W) \to \mathcal{M}_G(V)$ *is of type II relative to* φ.

Proof. Uniqueness follows from the fact that the composition

$$\ker X(D_\varphi) \hookrightarrow X(T_W) \overset{N_\varphi^{-1}X(D_\varphi)}{\longrightarrow} X(T_V)$$

is trivial. It remains to find a decomposition for γ. Choose decompositions $X(T_W) = \ker X(D_\varphi) \oplus A$ and $X(T_V) = \operatorname{im} N_\varphi^{-1}X(D_\varphi) \oplus B$. Define the homomorphisms $\alpha, \beta\colon X(T_W) \to \mathcal{M}_G(V)$ by

$$\alpha|_{\ker X(D_\varphi)} = 1,\ \beta|_{\ker X(D_\varphi)} = \gamma|_{\ker X(D_\varphi)} \quad \text{and} \quad \alpha|_A = \gamma|_A,\ \beta|_A = 1.$$

Clearly β is of type II relative to φ and $\alpha\beta = \gamma$.

Note that the homomorphism $N_\varphi^{-1}X(D_\varphi)\colon X(T_W) \to X(T_V)$ induces an isomorphism from A to its image in $X(T_V)$. Thus we may define $\varepsilon\colon X(T_V) \to \mathcal{M}_G(V)$ by $\varepsilon|_B = 1$ and $\varepsilon(N_\varphi^{-1}X(D_\varphi)(\chi)) = \gamma(\chi)$ for $\chi \in A$. This shows that α is of type I relative to φ, finishing the proof. □ □

In the sequel the following Lemma will be useful:

Lemma 11. *If γ is of type I relative to φ then $\overline{(\gamma\varphi)(V_{\bar{k}})} \subseteq \overline{\varphi(V_{\bar{k}})}$ and in particular $\dim(\gamma\varphi) \leq \dim\varphi$. For arbitrary γ the dimension of $\gamma\varphi$ is at most $\dim\varphi + (\operatorname{rk} X(T_W) - \operatorname{rk} M_\varphi)$.*

Proof. Let γ be of type I relative to φ. Hence there exists $\varepsilon\colon T_V \to \mathcal{M}_G(V)$ such that $\gamma = \varepsilon \circ N_\varphi^{-1}X(D_\varphi)$. We have rational evaluation maps $\operatorname{ev}_\gamma\colon \mathbb{A}(V) \dashrightarrow T_W$ and $\operatorname{ev}_\varepsilon\colon \mathbb{A}(V) \dashrightarrow T_V$, such that $\operatorname{ev}_\gamma(v) = (f_1(v), \ldots, f_n(v))$ where f_j is the image of the j-th standard basis vector under γ in $\mathcal{M}_G(V)$, and similiarly for ε. Now let $v \in V_{\bar{k}}$ such that $\operatorname{ev}_\varepsilon$ and φ are defined in v. Choose $t \in T_V(\bar{k})$ such that $t^{N_\varphi} = \operatorname{ev}_\varepsilon(v)$. Then one checks easily that $\operatorname{ev}_\gamma(v) = D_\varphi(t)$, whence

$$(\gamma\varphi)(v) = \operatorname{ev}_\gamma(v)\varphi(v) = D_\varphi(t)\varphi(v) = \varphi(tv).$$

This proves the first claim.

The second claim follows from the first, since the image of $\ker X(D_\varphi) \hookrightarrow X(T_W) \to \mathcal{M}_G(V)$ is generated by $r := \operatorname{rk}(\ker X(D_\varphi)) = \operatorname{rk} X(T_W) - \operatorname{rk} M_\varphi$ functions. □ □

3. Properties of multihomogeneous covariants

3.1. **The rank of the degree-matrix of a multihomogeneous covariant.** Let G be semi-faithful and $V = \bigoplus_{i=1}^m V_i, W = \bigoplus_{j=1}^n W_j$ be two faithful representations of G. For a faithful multihomogeneous covariant $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ we will prove the following interpretation of the rank of the degree-matrix M_φ:

Theorem 12. *Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant. Assume that $W_1, \ldots, W_n$ are irreducible.*

$$\operatorname{edim}_k G - \operatorname{rk} Z(G,k) \leq \dim\varphi - \operatorname{rk} M_\varphi.$$

If furthermore $V_1, \ldots, V_n$ are irreducible then

$$\operatorname{rk} M_\varphi \geq \operatorname{rk} Z(G,k)$$

with equality if φ is minimal.

Proof. Let $Z := Z(G,k)$. We first prove the second inequality. Since φ is at the same time equivariant with respect to the tori- and G-action $g\varphi(v) = \varphi(gv) = (D_\varphi g)\varphi(v)$ for $g \in Z$. Thus the map D_φ is the identity restricted to Z. This implies $Z = D_\varphi(Z) \subset D_\varphi(T)$, whence $\operatorname{rk} M_\varphi = \dim D_\varphi(T) \geq \operatorname{rk} Z$. The first inequality follows from the following: □ □

Proposition 13. *Let $\varphi = (\varphi_1, \dots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful rational multihomogeneous covariant. Assume that each W_j in the decomposition of W is irreducible. If $\operatorname{rk} M_\varphi \geq \operatorname{rk} Z(G,k)$ there exists a sub-torus $S \subseteq D_\varphi(T_V)$ of dimension $\operatorname{rk} M_\varphi - \operatorname{rk} Z(G,k)$ and a G-invariant open subset $W' \subseteq \mathbb{A}(W)$ on which $D_\varphi(T_V)$ acts freely such that the action of G on the quotient $(\overline{\operatorname{im}\varphi} \cap W')/S$ is faithful.*

Proof. Let $Z := Z(G,k)$. The torus $D_\varphi(T_V)$ has dimension $d := \operatorname{rk} M_\varphi \geq r := \operatorname{rk} Z$. By the elementary divisor theorem there exist integers $c_1, \dots, c_r > 1$ and a basis $\chi_1, \dots, \chi_d$ of $X(D_\varphi(T_V))$ such that

$$Z = \bigcap_{i=1}^{r} \ker \chi_i^{c_i} \cap \bigcap_{j=r+1}^{d} \ker \chi_j.$$

Set $S := \bigcap_{i=1}^{r} \ker \chi_i$. This is a subtorus of $D_\varphi(T_V)$ of rank $d - r = \operatorname{rk} M_\varphi - \operatorname{rk} Z$ with $S \cap Z = \{1\}$.

Let $W' := \prod_{j=1}^{n} W_j'$, where $W_j' := \mathbb{A}(W_j) \setminus \{0\}$ if $\varphi_j \neq 0$ and $W_j' := \mathbb{A}(W_j)$ otherwise. Our convention that $(M_\varphi)_{ij} = 0$ if $\varphi_j = 0$ implies that $D_\varphi(T_V)$ (and therewith S) acts freely on W'. Let $X := \overline{\operatorname{im}(\varphi)}$ and set $X' := X \cap W'$. Let $\pi\colon \mathbb{A}(W) \dashrightarrow W'/S$ be the rational projection map. The kernel of the action of G on X'/S is contained in $Z(G,k)$ by the next lemma. Since $Z(G,k) \cap S = \{e\}$ it is trivial. Hence the rational map $\mathbb{A}(V) \overset{\varphi}{\dashrightarrow} X \dashrightarrow X'/S$ is a compression and $\operatorname{edim}_k G \leq \dim X'/S = \dim X - \dim S = \dim \varphi - (\operatorname{rk} M_\varphi - \operatorname{rk} Z)$. □ □

Lemma 14. *Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a faithful multihomogeneous covariant. Let $P := \prod_{j:\varphi_j \neq 0} \mathbb{P}(W_j) \times \prod_{j:\varphi_j = 0} \mathbb{A}(W_j)$ and $\pi\colon \mathbb{A}(W) \dashrightarrow P$ the obvious G-equivariant rational map and let $X := \overline{\operatorname{im}\varphi}$. Then the kernel Q of the action of G on $\pi(X)$ equals $Z(G,k)$.*

Proof. The elements of the k-center $Z(G,k)$ act as scalar on $\mathbb{A}(W_j)$ for each j. This implies that $Z(G,k)$ is contained in Q. Conversely let $g \in Q$ and fix some $j \in \{1, \dots, n\}$ with $\varphi_j \neq 0$. We want to show that g acts by multiplication of a (fixed) scalar on W_j. From this the inclusion $Q \subseteq Z(G,k)$ follows, since $\bigoplus_{j:\varphi_j \neq 0} W_j$ is already a faithful completely reducible representation of G.

Let $Y \subseteq \mathbb{A}(W_j)$ denote the projection of $X \cap W'$ to $\mathbb{A}(W_j)$. Since g acts trivially on $\pi(X)$ there exists for every field extension k'/k and $y \in Y(k')$ some $\lambda_y \in \mathbb{G}_m(k')$ such that $gy = \lambda_y y$. Since g has only finitely many eigenvalues $\alpha_1, \dots, \alpha_r \in \mathbb{G}_m(\bar{k})$ the same holds for its closure $\overline{Y}$. Moreover since $\overline{Y}$ is irreducible the scalar $\lambda := \lambda_y$ does not depend on y. Since $\varphi_j \neq 0$ the variety $\overline{Y}$ contains a non-zero $k(V)$-rational point y_0. By irreducibility of $W_j \otimes k(V)$ the set $\{g'y_0 \mid g' \in G\}$ spans $W_j \otimes k(V)$ as a $k(V)$-vector space. It follows that g acts by multiplication of λ on $W_j \otimes k(V)$, hence in the same manner on W_j, which completes the proof. □ □

To illustrate the usefulness of the existence of minimal faithful multihomogeneous covariants and Lemma 14 we give a simple corollary. Its first part was already established in [BR97, Theorem 6.1].

Corollary 15. *Let A be abelian and assume that k contains a primitive root of unity of order* $\exp A$. *Then*

$$\operatorname{edim}_k A = \operatorname{rk} A.$$

If G is semi-faithful and if $\operatorname{edim}_k G \leq \operatorname{rk} Z(G,k) + 1$, then G is an extension of a subgroup of $\mathrm{PGL}_2(k)$ by $Z(G,k)$.

If $\operatorname{edim}_k G \leq \operatorname{rk} Z(G,k)$ then $G = Z(G,k)$, hence abelian with $\zeta_{\exp G} \in k$.

Proof. The inequality $\operatorname{edim}_k A \leq \operatorname{rk} A$ is easy to see, because A has a faithful representation of dimension $\operatorname{rk} A$. Let V be a completely reducible faithful representation of G and let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal faithful multihomogeneous covariant of G. We may assume that $\varphi_j \neq 0$ for all j. The group $G/Z(G,k)$ then acts faithfully on the image of $\pi_V \circ \varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V) \dashrightarrow \mathbb{P}(V)$, which has dimension at most $\dim \varphi - \operatorname{rk} Z(G,k) = \operatorname{edim}_k G - \operatorname{rk} Z(G,k) \leq 1$. Thus $G/Z(G,k)$ embeds into $\mathrm{PGL}_2(k)$. Now if $\operatorname{edim}_k G \leq \operatorname{rk} Z(G,k)$ then $\operatorname{edim}_k G = \operatorname{rk} Z(G,k)$ and the image of $\pi_V \circ \varphi$ must be a point, whence $G = Z(G,k)$. □ □

Remark 1. The second part of Corollary 15 can be used to classify semi-faithful groups with $\operatorname{edim}_k G - \operatorname{rk} Z(G,k) \leq 1$. For example if $\operatorname{edim}_k G \leq 2$ and $Z(G,k)$ is nontrivial one should obtain with the arguments of [KS07, section 10] that $G \hookrightarrow \mathrm{GL}_2(k)$. We haven't checked that in detail, but one observes that the additional possibilities for subgroups of $\mathrm{PGL}_2(k)$ arising in positive characteristic are not semi-faithful.

3.2. **Behavior under refinement of the decomposition.** Let $V = \bigoplus_{i=1}^m V_i$ be a graded vector space. For each i let $V_i = \bigoplus_{k=1}^{d_i} V_{ik}$ be a grading of V_i. We call the grading $V = \bigoplus_{i,k} V_{ik}$ a *refinement* of the grading $V = \bigoplus_i V_i$. Let $\varphi = (\varphi_1, \ldots, \varphi_n)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ be a multihomogeneous rational map. We consider refinements both in V and in $W = \bigoplus_{j=1}^n W_j$ where $W_j = \bigoplus_{l=1}^{e_j} W_{jl}$, and study the behavior of the rank of the degree matrix. Set $d = \sum_{i=1}^m d_i$ and $e = \sum_{j=1}^n e_j$.

Proposition 16. (A) *Refinement in V: Let λ be a one-parameter subgroup of $T_V = \mathbb{G}_m^d$ such that $H_\lambda(\varphi)\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is multihomogeneous w.r.t. the refined grading on V and the old grading on W. Then*

$$\operatorname{rk} M_{H_\lambda(\varphi)} \geq \operatorname{rk} M_\varphi.$$

(B) *Refinement in W: The map φ can be considered as a multihomogeneous map $\varphi'\colon \mathbb{A}(V) \to \mathbb{A}(W)$ with respect to the gradings $V = \bigoplus_i V_i$ and $W = \bigoplus_{jl} W_{jl}$, where*

$$\operatorname{rk} M_{\varphi'} = \operatorname{rk} M_\varphi.$$

(C) *Refinement in both V and W: Consider φ' as above and let λ be a one-parameter subgroup of $T_V = \mathbb{G}_m^d$ be such that $H_\lambda(\varphi')\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W)$ is multihomogeneous w.r.t. the refined grading on both V and W. Then*

$$\operatorname{rk} M_{H_\lambda(\varphi')} \geq \operatorname{rk} M_\varphi.$$

Proof. (A) Let $(a_{i,j}) = M_\varphi \in \mathcal{M}_{m,n}(\mathbb{Z})$ and $(b_{ik,j}) = M_{H_\lambda(\varphi)} \in \mathcal{M}_{d,n}(\mathbb{Z})$ be the degree matrices of φ and $H_\lambda(\varphi)$, respectively. Since $H_\lambda(\varphi)$ is still multihomogeneous with respect to the old decomposition of V we have $\sum_{k=1}^{d_i} b_{ik,j} = a_{i,j}$ for $i = 1 \ldots m$ and $j = 1 \ldots n$. Therefore the span of the rows of $M_{H_\lambda(\varphi)}$ contains the span of the rows of M_φ. Hence $\operatorname{rk} M_{H_\lambda(\varphi)} \geq \operatorname{rk} M_\varphi$.

(B) The maps $\varphi_{jl}\colon V \dashrightarrow W_{jl}$ are still multihomogeneous of the same degree as $\varphi_j\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(W_j)$, as long as they are non-zero. If φ_j is non-zero then also one of the φ_{jl} for $l = 1 \ldots e_j$. Recall that by convention the

matrix entries for zero-components are zero, so that they do not influence the column span of the matrix. Thus the column span of M_φ equals the column span of $M_{\varphi'}$ and hence $\operatorname{rk} M_\varphi = \operatorname{rk} M_{\varphi'}$.

(C) follows from (A) and (B).

□ □

4. Completely reducible faithful representations

4.1. **Minimal number of irreducible components.** In this section we will compute the minimal number of irreducible components of a faithful representation of any semi-faithful group. As a consequence we obtain a characterization of groups, which have a faithful representation with any fixed number of irreducible components. Groups admitting an irreducible faithful representation over an algebraically closed field of characteristic 0 have been characterized in [Ga54]. A criterion for a group to admit a faithful representation with any fixed number of irreducible components was given by Shoda [Sh30] (in the ordinary case) and Nakayama [Na47] (in the modular case). Their criterion is formulated in a way quite different from Gaschuetz's and our characterization.

Definition 7. A *foot* of G is a minimal nontrivial normal subgroup of G. The subgroup of G generated by the (abelian) feet of G is called the (abelian) *socle of* G, denoted by $\operatorname{soc}(G)$ (resp. $\operatorname{soc}^{\mathrm{ab}}(G)$).

By construction $\operatorname{soc}(G)$ and $\operatorname{soc}^{\mathrm{ab}}(G)$ are normal. The following Lemma is well known and a generalization to countable groups can be found in [BH08].

Lemma 17. $\operatorname{soc}(G) = \operatorname{soc}^{\mathrm{ab}}(G) \times N_1 \times \cdots \times N_r$, *where* $N_1, \dots, N_r$ *are all the non-abelian feet of* G.

For a $\mathbb{Z}G$-module A denote by $\operatorname{rk}_{\mathbb{Z}G}(A)$ the minimum number of generators:

$$\operatorname{rk}_{\mathbb{Z}G}(A) := \min\{r \in \mathbb{N}_0 \mid \exists a_1, \dots, a_r \in A : \langle a_1, \dots, a_r\rangle_{\mathbb{Z}G} = A\} \in \mathbb{N}_0.$$

Proposition 18. *Let* G *be a semi-faithful group. Then the minimal number of factors of a decomposition series of a faithful representation of* G *over* k *equals* $\operatorname{rk}_{\mathbb{Z}G} \operatorname{soc}^{\mathrm{ab}}(G)$ *if* $\operatorname{soc}^{\mathrm{ab}}(G) \neq \{e\}$ *and* 1 *if* $\operatorname{soc}^{\mathrm{ab}}(G)$ *is trivial. Moreover the minimum is attained by a completely reducible representation.*

We start with a lemma explaining how to pass from arbitrary to completely reducible representations.

Lemma 19. *Let* V *be a faithful representation of* G *and* $\mathcal{F} = V = V_1 \supsetneq V_2 \supsetneq \cdots \supsetneq V_r \supsetneq V_{r+1} = \{0\}$ *be a* G*-stable flag. Assume that* $\operatorname{char} k = p > 0$. *If* G *does not contain a nontrivial normal subgroup of* p*-power order then the associated graded representation* $\operatorname{gr}_{\mathcal{F}} V = \bigoplus_{i=1}^{r} V_i/V_{i+1}$ *is faithful as well. In particular such a group* G *is semi-faithful (over* k*).*

Proof. It is well known that an element of finite order in a unipotent group in characteristic p has p-power order. Therefore the kernel of the representation $\operatorname{gr}_{\mathcal{F}} V$ is a normal subgroup of G of p-power order, which by assumption must be trivial. The last statement follows from taking for $\mathcal{F}$ a decomposition series. □ □

For the proof of Proposition 18 we work with two lattices: Set $A := \operatorname{soc}^{\mathrm{ab}}(G)$ and let $A^* := \operatorname{Hom}(A, \bar{k}^*)$ denote its group of characters over $\bar{k}$, which is again a $\mathbb{Z}G$-module by endowing $\bar{k}^*$ with the trivial G-action. Denote by $L(A)$ and $L(A^*)$

the lattices of $\mathbb{Z}G$-invariant subspaces of A and A^*, respectively, where the meet-operation is given by $B \cap C$ and the join-operation by $B \cdot C$.

Lemma 20. *Assume that either* $\operatorname{char} k = 0$ *or* $\operatorname{char} k = p > 0$ *and* $p \nmid |A|$.

(A) *The map*

$$\alpha \colon L(A^*) \to L(A), \quad \mathcal{L} \mapsto \{a \in A \mid \ell(a) = 1 \ \forall \ell \in \mathcal{L}\}$$

yields an anti-isomorphism of $L(A^*)$ *and* $L(A)$ *with inverse given by* $\alpha^{-1}(B) = \{\ell \in A^* \mid \ell(a) = 1 \ \forall a \in A\}$.

(B) *There exists a (non-canonical) isomorphism of lattices*

$$\beta \colon L(A) \xrightarrow{\simeq} L(A^*)$$

which preserves size, i.e. $|\beta(B)| = |B|$ *for all* $B \in L(A)$.

(C) $\operatorname{rk}_{\mathbb{Z}G}(A) = \operatorname{rk}_{\mathbb{Z}G}(A^*)$.

Proof. (A) The proof is straightforward.

(B) The $\mathbb{Z}G$-module A is semi-simple by construction and thus decomposes into isotypic components. Every submodule of A is isomorphic to the direct sum of its intersections with the isotypic components and it suffices to show the claim for every isotypic component of A. Thus assume $A = (\mathbb{F}_q)^m \otimes V$ for some prime $q \neq \operatorname{char} k$, some natural number m and some irreducible $\mathbb{F}_q G$-module V, where $(\mathbb{F}_q)^m$ is equipped with the trivial action of G. Hence we may identify $A^* = (\mathbb{F}_q)^m \otimes V^*$. Every $\mathbb{Z}G$-invariant subgroup of A is now of the form $W \otimes V$ for some sub vector-space $W \subset \mathbb{F}_q^m$. Define $\beta \colon L(A) \to L(A^*)$ by $\beta(W \otimes V) = W \otimes V^*$. Then β is an isomorphism of lattices and preserves size, since the assumption $p \nmid |A|$ implies $|V^*| = |V|$.

(C) Let $E_r \subseteq A$ for $r \in \mathbb{N}$ denote the (possibly empty) set of generating r-tuples of the $\mathbb{Z}G$-module A and let $\max(L(A))$ be the set of maximal non-trivial elements of $L(A)$. The two sets are related by:

$$E_r = A^r \setminus \bigcup_{M \in \max(L(A))} M^r.$$

Similarly for $E_r^* \subseteq A^*$ and $\max(L(A^*))$ defined correspondingly with A^* in place of A we have

$$\begin{aligned} E_r^* &= (A^*)^r \setminus \bigcup_{\mathcal{L} \in \max(L(A^*))} \mathcal{L}^r \\ &= (\beta(A))^r \setminus \bigcup_{M \in \max(L(A))} (\beta(M))^r \end{aligned}$$

We claim for any r that $|E_r| = |E_r^*|$. This implies in particular that A is generated by r elements if and only if A^* is, hence $\operatorname{rk}_{\mathbb{Z}G}(A) = \operatorname{rk}_{\mathbb{Z}G}(A^*)$. The claim follows from part (B) and the exclusion principle, which says that for subsets $Y_1, \ldots, Y_t$ of a set Y we have

$$|Y \setminus \cup_{i=1}^t Y_i| = |Y| - \sum_{i=1}^{t} (-1)^{t+1} \sum_{\nu_1 < \cdots < \nu_i} |Y_{\nu_1} \cap \cdots \cap Y_{\nu_i}|$$

□ □

For the case that k is not algebraically closed, we need to deal with irreducible representations which are not absolutely irreducible:

Lemma 21. (A) *Let $q \neq \operatorname{char} k$ be a prime and A be an elementary abelian q-group. Then each non-trivial irreducible representation of A (over k) is isomorphic to a sub-representation of*

$$V_{\langle\chi\rangle} := \left\{ \sum_{C\in A/\ker\chi} \gamma_C(\sum_{a\in C} a) \in kA \mid \sum_{C\in A/ker\chi} \gamma_C = 0 \right\}$$

where $\chi \in \operatorname{Hom}(A, \bar{k}^*)$, $\chi \neq 1$.

(B) *Let $A = \bigoplus_{i=1}^m A_{q_i}$ where $q_1, \dots, q_m \neq \operatorname{char} k$ are distinct primes and A_{q_i} is an elementary abelian q_i group. Then every irreducible representation V of A is an exterior tensor product of irreducible representations of $A_{q_1}, \dots, A_{q_m}$. Let $\chi_1, \dots, \chi_r$ be the characters appearing in $V \otimes_k \bar{k}$. Then $\langle\chi_1, \dots, \chi_r\rangle = \langle\chi_i\rangle$ for every $i = 1 \dots r$.*

Proof. (A) It suffices to show that the group algebra kA decomposes as

$$\bigoplus_{\langle\chi\rangle\subseteq\operatorname{Hom}(A,\bar{k}^*)} V_{\langle\chi\rangle},$$

where we set $V_{\langle\chi\rangle} = k\sum_{a\in A} a$ for $\chi = 1$, which has dimension one. Let $n := \dim_{\mathbb{F}_q} A$. There are precisely $\frac{q^n-1}{q-1}$ nontrivial subgroups of the form $\langle\chi\rangle$ and the corresponding subspaces $V_{\langle\chi\rangle}$ all have dimension $q-1$. Since $(q-1)\cdot\frac{q^n-1}{q-1} + 1\cdot 1 = q^n = |A| = \dim_k kA$ it remains to show that the subspaces $V_{\langle\chi\rangle}$ form a direct sum, for which we may pass to an algebraic closure. Consider the elements $\varepsilon_\chi := \sum_{a\in A}\chi(a^{-1})a \in \bar{k}A$ for $\chi \in \operatorname{Hom}(A, \bar{k}^*)$, which are $\bar{k}$-linearly independent. Then $V_{\langle\chi\rangle} \otimes \bar{k}$ has $\bar{k}$-basis $\varepsilon_\chi, \dots, \varepsilon_{\chi^{q-1}}$ for $\chi \neq 1$ and $V_{\langle 1\rangle}$ has basis ε_0. That shows the claim.

(B) Writing $kA = kA_{q_1} \otimes \cdots \otimes kA_{q_m}$ the first claim follows from the fact that the group algebras kA_{q_i} are of coprime dimensions. The second claim follows now from the description in (A), noting that the representation $V_{\langle\chi\rangle}$ has character $\sum_{i=1}^{q-1}\chi^i$.

□ □

The following lemma contains the crucial observation for our study of faithful representations.

Lemma 22. *Let $V = \bigoplus_{i=1}^m V_i$ be a representation of G with each V_i irreducible. Let $A := \operatorname{soc}^{\mathrm{ab}}(G)$ and choose for every i some character $\chi_i \in A^*$ appearing in $V_i|_A \otimes \bar{k}$. Then V is faithful if and only if the characters $\chi_1, \dots, \chi_m$ generate A^* as a $\mathbb{Z}G$-module and no nonabelian foot of G is in the kernel of V.*

Proof. Let $\mathcal{L} := \langle\chi_1, \cdots, \chi_m\rangle_{\mathbb{Z}G} \in L(A^*)$. Assume that $\mathcal{L} \neq A^*$. Let α be the lattice anti-isomorphism from Lemma 20(A) and set $B := \alpha(\mathcal{L}) \subseteq A$, which is then a non-trivial normal subgroup of A contained in the kernel of each χ_i and of any power of χ_i. Let W_i be any irreducible sub-representation of $V_i|_A$ containing the character χ_i. By Lemma 21 $W_i \otimes \bar{k} = \sum \bar{k}_{\chi_i^{\alpha_{ij}}}$ for some $\alpha_{ij} \in \mathbb{N}$. Therefore B acts trivially on W_i. Now since V_i is irreducible, $V_i = \sum_{g\in G} gW_i$ as vector spaces. For $b \in B$ and $w \in W_i$ we have $bgw = g(g^{-1}bg)w = gw$, since B is normal. Thus B acts trivially on V. Hence V is not faithful.

Conversely assume that V is not faithful and no noabelian foot of G is in the kernel of V. Hence some abelian foot B is in the kernel of V. This implies that B

lies in the kernel of each χ_i, whence in the kernel of each element of $\mathcal{L}$. This implies that $\mathcal{L} \neq A^*$. □ □

Now we are ready for the proof of the proposition.

Proof of Proposition 18. : Recall that a group admitting a nontrivial normal subgroup of p-power order is not semi-faithful in characteristic p. From now on assume that $p \nmid |A|$ where $A := \mathrm{soc}^{\mathrm{ab}}(G)$.

"$\geq$" Let V be a faithful representation of G over k. We want to show that the number of factors of a decomposition series of V is at least the maximum of $\mathrm{rk}_{\mathbb{Z}G}(A)$ and 1. Clearly it is at least 1. By Lemma 19 we may assume that V is completely reducible. Lemma 22 implies that the number of irreducible components of V is at least $\mathrm{rk}_{\mathbb{Z}G}(A^*)$, which equals $\mathrm{rk}_{\mathbb{Z}G}(A)$ by Lemma 20(C).

"$\leq$" We must construct a faithful representation V over k with at most $\mathrm{rk}_{\mathbb{Z}G}(A)$ irreducible components if A is non-trivial, and a faithful irreducible representation V over k if A is trivial. We first reduce to the case of k being algebraically closed: Assume that $\bigoplus_{i=1}^n V_i$ is a decomposition of a faithful representation into irreducible representations over $\bar{k}$. For each i take any irreducible representation V_i' over k which contains V_i as a decomposition factor over $\bar{k}$. Then $\bigoplus_{i=1}^n V_i'$ is a faithful representation over $\bar{k}$ and has the same number of irreducible components.

Let $N_1, \ldots, N_t$ be the non-abelian feet of G. By Lemma 17 the socle of G decomposes as $\mathrm{soc}\, G = A \times N_1 \times \ldots \times N_t$. For each i, since N_i has composite order it has a nontrivial irreducible representation W_i. The (exterior) tensor product $W := W_1 \otimes \cdots \otimes W_t$ is then irreducible (since $k = \bar{k}$) and does not contain any of $N_1, \cdots, N_t$ in its kernel. If A is trivial this gives an irreducible representation of $\mathrm{soc}\, G$ with the property that no foot of G is contained in its kernel. Any irreducible representation whose restriction to $\mathrm{soc}\, G$ contains W is then faithful.

From now on assume A to be non-trivial. There exist $r := \mathrm{rk}_{\mathbb{Z}G}(A^*) = \mathrm{rk}_{\mathbb{Z}G}(A)$ characters $\chi_1, \ldots, \chi_r$ of A which generate the $\mathbb{Z}G$-module A^*. For every i choose an irreducible representation V_i of G whose restriction to $\mathrm{soc}\, G$ contains the irreducible representation $k_{\chi_i} \otimes W$. Set $V := \bigoplus_{i=1}^r V_i$. By Lemma 22 the representation V is faithful. Moreover it has the required number of irreducible components. This finishes the proof.

□ □

Remark 2. The situation for non-semi-faithful groups is completely different, in so far that the abelian socle tells nothing about the number of decomposition factors needed for a faithful representation. Take for example the groups $\mathbb{Z}/p^n\mathbb{Z}$, $n \geq 1$, whose abelian socle are all isomorphic although for large n these groups need more than any fixed number of decomposition factors for a faithful representation.

Remark 3. More generally let Γ be any subgroup of $\mathrm{Aut}(G)$ containing the inner automorphisms. One can define Γ-faithful representations, Γ-feet, Γ-socle, abelian Γ-socle (denoted in the sequel by $A^\Gamma(G)$) as in [BH08] and generalize Proposition 18 in the following way: If $\mathrm{char}\, k = 0$ or $\mathrm{char}\, k = p > 0$ and $p \nmid |A^\Gamma(G)|$ then the minimal number of irreducible components of a completely reducible Γ-faithful

representation of G equals the maximum of $\mathrm{rk}_{\mathbb{T}} A^\Gamma(G)$ and 1. The proof remains basically the same.

There is the following application:

Corollary 23. *Let $n \in \mathbb{N}$ and $H \subseteq G$ be a subgroup containing $\mathrm{soc}^{\mathrm{ab}}(G)$ and assume that H has a faithful representation over k with n decomposition factors. If $\mathrm{char}\, k \nmid |\mathrm{soc}^{\mathrm{ab}}(G)|$ then G has a faithful representation with n decomposition factors as well.*

Proof. This is a consequence of the following Lemma 24 together with Proposition 18. Observe that $\mathrm{char}\, k \nmid |\mathrm{soc}^{\mathrm{ab}}(G)|$ implies that $\mathrm{char}\, k \nmid |\mathrm{soc}^{\mathrm{ab}}(H)|$, hence both groups are semi-faithful. □ □

Lemma 24. *If $H \subseteq G$ is a subgroup containing $\mathrm{soc}^{\mathrm{ab}}(G)$ then $\mathrm{rk}_{\mathbb{Z}H} \mathrm{soc}^{\mathrm{ab}}(H) \geq \mathrm{rk}_{\mathbb{Z}G} \mathrm{soc}^{\mathrm{ab}}(G)$.*

Proof. Let $h_1, \ldots, h_r$ generate $\mathrm{soc}^{\mathrm{ab}}(H)$ as a $\mathbb{Z}H$-module, where $r = \mathrm{rk}_{\mathbb{Z}H}(\mathrm{soc}^{\mathrm{ab}}(H))$. Let N be an H-invariant complement of $\mathrm{soc}^{\mathrm{ab}}(H) \cap \mathrm{soc}^{\mathrm{ab}}(G)$ in $\mathrm{soc}^{\mathrm{ab}}(H)$. Write $h_i = (g_i, n_i)$ where $n_i \in N$ and $g_i \in \mathrm{soc}^{\mathrm{ab}}(H) \cap \mathrm{soc}^{\mathrm{ab}}(G)$. Then $g_1, \ldots, g_r$ generate $\mathrm{soc}^{\mathrm{ab}}(H) \cap \mathrm{soc}^{\mathrm{ab}}(G)$ as a $\mathbb{Z}H$-module. We show that $g_1, \ldots, g_r$ generate $\mathrm{soc}^{\mathrm{ab}}(G)$ as a $\mathbb{Z}G$-module, which gives the claim. Let A be any abelian foot of G. By assumption $A \subseteq \mathrm{soc}^{\mathrm{ab}}(G) \subseteq H$. Let $B \subseteq A$ be a H-foot. By construction $B \subseteq \mathrm{soc}^{\mathrm{ab}}(H) \cap \mathrm{soc}^{\mathrm{ab}}(G)$, which is generated by $g_1, \ldots, g_r$ as a $\mathbb{Z}H$-module. Since A is minimal, the $\mathbb{Z}G$-module generated by B equals A. Hence A is contained in the $\mathbb{Z}G$-module generated by $g_1, \ldots, g_r$. Since this holds for every abelian foot A of G the claim follows. □ □

There is a simple lower bound on the number of irreducible components needed for a faithful representation, namely the rank of the center of G. Since representations for which the bound is reached are of some special interest later, we give it a name:

Definition 8. A faithful representation V of a semi-faithful group G is called *saturated* if it is the direct sum of $\mathrm{rk}\, Z(G)$ many irreducible representations of G.

The group G is called *saturated* if it has a (faithful) saturated representation. Equivalently (by Proposition 18):

$$\mathrm{rk}\, Z(G) = \mathrm{rk}_{\mathbb{Z}G} \mathrm{soc}^{\mathrm{ab}}(G) \geq 1.$$

It is sometimes advantageous to pass to saturated groups by taking the product with cyclic groups of high enough rank:

Proposition 25. *Let $\ell \neq \mathrm{char}\, k$ be any prime number such that $\zeta_\ell \in k$. Assume that G has a completely reducible faithful representation $V = \bigoplus_{i=1}^n V_i$, each V_i irreducible. Let r be the rank of the ℓ-Sylow subgroup of $Z(G)$. Then V carries a faithful representation of $G \times C_\ell^{n-r}$.*

Proof. We proceed by induction on $n - r$. If $n - r = 0$ there is nothing to show. Otherwise $r < n$ and there exists $i \in \{1, \ldots, n\}$ such that no element of G acts by multiplication of a primitive ℓ-th root of unity on V_i and trivially at the same time on every V_j for $j \neq i$. Thus letting C_ℓ act by multiplication of ζ_p on V_i and trivially on V_j for $j \neq i$ yields a faithful representation of $\tilde{G} := G \times C_\ell$ on V. Now apply the induction hypothesis to $\tilde{G}$. □ □

4.2. **Minimal dimension of faithful representations.** We define the *representation dimension* of G over k as follows:

Definition 9. $\operatorname{rdim}_k G := \min\{\dim V \mid V \text{ faithful representation of } G \text{ over } k\}$.

This new numerical invariant gives an upper bound for $\operatorname{edim}_k G$. In certain cases the two invariants of G coincide, e.g. for p-groups when k contains a primitive p-th root of unity, see [KM08, Theorem 4.1].

Definition 10. Let A be an abelian subgroup of G and $\chi \in A^* := \operatorname{Hom}(A, \bar{k}^*)$.

$$\operatorname{rep}^{(\chi)}(G) := \{V \text{ irreducible representation of } G \mid (V \otimes \bar{k})|_A \supseteq \bar{k}_\chi\},$$

where $\bar{k}_\chi$ is the one-dimensional representation of A over $\bar{k}$ on which A acts via χ.

To every group G and field k we associate the following function:

$$f_{G,k} \colon A^* \to \mathbb{N}_0, \quad \chi \mapsto \min\{\dim V \mid V \in \operatorname{rep}^{(\chi)}(G)\},$$

where $A = \operatorname{soc}^{\mathrm{ab}}(G)$.

From Lemma 22 we get the following

Corollary 26. *If the socle $C = \operatorname{soc} G$ of G is abelian and $\operatorname{char} k \nmid |C|$, then*

$$\operatorname{rdim}_k G = \min\left\{\sum_{i=1}^{r} f_{G,k}(\chi_i)\right\}$$

taken over all $r \in \mathbb{N}$ and all systems of generators $(\chi_1, \ldots, \chi_r)$ of C^* viewed as a $\mathbb{Z}G$-module.

It may happen that every faithful representation of minimal dimension has more decomposition factors than needed in minimum to create a faithful representation. However in the following situation that doesn't occur and we can describe faithful representations of minimal dimensions more precisely. Recall the definition of a minimal basis introduced in [KM08]:

Definition 11. Let C be a vector space over some field F of dimension $r \in \mathbb{N}_0$ and let $f \colon C \to \mathbb{N}_0$ be any function. An F-basis $(c_1, \ldots, c_r)$ of C is called *minimal relative to f* if

$$f(c_i) = \min\left\{f(c) \mid c \in C \setminus \langle c_1, \ldots, c_{i-1}\rangle\right\}, \tag{3}$$

for $i = 1, \ldots, r$ where for $i = 1$ we use the convention that the span of the empty set is the trivial vector space $\{0\}$.

Proposition 27. *Let G be a group whose socle $C := \operatorname{soc} G$ is a central p-subgroup for some prime p and assume $\operatorname{char} k \neq p$. Let V be any representation of G and let $V_1, V_2, \ldots, V_r$ be its irreducible composition factors ordered increasingly by dimension. Choose characters $\chi_1, \ldots, \chi_r \in C^* = \operatorname{Hom}(C, \bar{k}^*)$ such that $V_i \in \operatorname{rep}^{(\chi_i)}(G)$. Then V is faithful of dimension $\operatorname{rdim}_k G$ if and only if $r = \operatorname{rk} C$ and $(\chi_1, \ldots, \chi_r)$ forms a minimal basis of $(C^*, f_{G,k})$ with $f_{G,k}(\chi_i) = \dim V_i$. The dimension vector $(\dim V_1, \ldots, \dim V_r)$ is unique amongst faithful representations of dimension $\operatorname{rdim}_k G$.*

Proof. Since $p \nmid |C|$ we may replace V by its associated graded representation $V_1 \oplus \ldots \oplus V_r$ without changing faithfulness, decomposition factors and dimension. Thus we will assume that V is completely reducible.

First assume that V is faithful and $\operatorname{rdim}_k G = \dim V$. Then the characters $\chi_1, \dots, \chi_r$ clearly generate C^* and in particular $r \geq \operatorname{rk} C$. Let $j \in \{0, \dots, r\}$ be maximal such that $(\chi_1, \dots, \chi_r)$ is part of a minimal basis of C^*. We want to show that $j = r$. Assume to the contrary that $j < r$. Hence there exists $\chi \in C^* \setminus \langle \chi_1, \dots \chi_j \rangle$ and $W \in \operatorname{rep}^{(\chi)}(G)$ such that $\dim W < \dim V_i$ for all $i > j$. By elementary linear algebra there exists $i > j$ such that $\chi_1, \dots, \chi_{i-1}, \chi, \chi_{i+1}, \dots, \chi_r$ generate C^* as well. Let $V' := V_1 \oplus \cdots V_{i-1} \oplus W \oplus V_{i+1} \oplus \cdots \oplus V_r$. Then $\dim V' < \dim V$ and V' is faithful, because V' is faithful restricted to C and every normal subgroup of G intersects $C = \operatorname{soc}(G)$. This contradicts to $\dim V = \operatorname{rdim}_k G$.

Now assume that $(\chi_1, \dots, \chi_r)$ and $(\chi'_1, \dots, \chi'_r)$ form two minimal bases of C^*. We show that $f_{G,k}(\chi_i) = f_{G,k}(\chi'_i)$ for all $i = 1 \dots r$. Let $j \in \{0, \dots, r\}$ be the last index where $(f_{G,k}(\chi_1), \dots, f_{G,k}(\chi_j))$ and $(f_{G,k}(\chi'_1), \dots, f_{G,k}(\chi'_j))$ coincide. Assume $j < r$ and assume $f_{G,k}(\chi'_{j+1}) < f_{G,k}(\chi_{j+1})$. Then $\langle \chi_1, \dots, \chi_j \rangle \neq \langle \chi'_1, \dots, \chi'_j \rangle$. Hence there exists $s \in \{1, \dots, j\}$ such that $\chi'_s \notin \langle \chi_1, \dots, \chi_j \rangle$. Then $f_{G,k}(\chi_{j+1}) > f_{G,k}(\chi'_{j+1}) \geq f_{G,k}(\chi'_s)$, which contradicts to the definition of minimal basis. This implies uniqueness of the dimension vector and the converse to the above implication. □ □

Remark 4. Under the assumptions of Proposition 27 let $(\chi_1, \dots, \chi_r)$ be a minimal basis of C^* and $1 \leq i_1 < i_2 < \cdots < i_m < r$ be the positions of jumps in the vector $(f_{G,k}(\chi_1), \dots, f_{G,k}(\chi_r))$, i.e. the indices i where $f_{G,k}(\chi_i) < f_{G,k}(\chi_{i+1})$. The argument in the proof of Proposition 27 shows that the subgroups $\langle \chi_1, \dots, \chi_{i_j} \rangle$ for $j = 1 \dots m$ do not depend on the choice of the minimal basis $(\chi_1, \dots, \chi_r)$. This yields a canonical filtration $C^* = A_{m+1} \supsetneq A_m \supsetneq \dots \supsetneq A_1 \supsetneq A_0 = \{e\}$ of C^* where $\operatorname{rk} A_j = i_j$ for $j = 1, \dots, m$. It would be interesting to know whether every basis $(\chi_1, \dots, \chi_r)$ of C^* respecting this grading of C^* is a minimal basis, or equivalently if for all $j = 0, \dots, m$ and $\chi, \chi' \in A_{j+1} \setminus A_j$ the equality $f_{G,k}(\chi) = f_{G,k}(\chi')$ holds.

Corollary 28. *Let p be a prime and $G_1, \dots, G_n$ be groups. Assume that* $\operatorname{char} k \neq p$ *and* $\operatorname{soc} G_i$ *is a central p-subgroup of G_i for $i = 1, \dots, n$. Then*

$$\operatorname{rdim}_k \prod_{i=1}^n G_i = \sum_{i=1}^n \operatorname{rdim}_k G_i.$$

The (statement and the) proof is very similar to [KM08, Theorem 5.1], which becomes a statement about minimal faithful representations of p-groups via [KM08, Theorem 4.1]. Since our situation is more general and we do not require k to contain a primitive p-th root of unity, we append the proof.

Proof. Using induction it suffices to show the case $n = 2$. Set $G := G_1 \times G_2$. Taking into account the description of minimal faithful representations of Proposition 27 it remains to create a minimal basis $(\chi_1, \dots, \chi_r)$ of $(\operatorname{soc} G)^* = (\operatorname{soc} G_1)^* \oplus (\operatorname{soc} G_2)^*$ for $f_{G,k}$ subject to the condition that each χ_i is contained in one of $(\operatorname{soc} G_i)^*$. Here $r = \operatorname{rk} Z(G) = \operatorname{rk} Z(G_1) + \operatorname{rk} Z(G_2)$. Assume that $(\chi_1, \dots, \chi_j)$ is part of a minimal basis such that each χ_i for $i \leq j$ is contained in one of $(\operatorname{soc} G_i)^*$. Choose $\chi \in (\operatorname{soc} G)^* \setminus \langle \chi_1, \dots, \chi_j \rangle$ with $f_{G,k}(\chi)$ minimal. Decompose χ as $\chi^{(1)} \oplus \chi^{(2)}$ where $\chi^{(i)} \in (\operatorname{soc} G_i)^*$ and choose $W \in \operatorname{rep}^{(\chi)}(G)$ of minimal dimension. The definition of $\operatorname{rep}^{(\chi)}(G)$ means that $\bar{k}_\chi \subseteq W \otimes \bar{k}$. Let ε_1 and ε_2 denote the endomorphism of G sending (g_1, g_2) to (g_1, e) and to (e, g_2), respectively. The representation $\rho_W \circ \varepsilon_i$ contains $\bar{k}_{\chi^{(i)}}$ and has the same dimension as W. Now replace χ by $\chi^{(i)}$ with i such

that $\chi^{(i)}$ lies outside the subgroup of $(\operatorname{soc} G)^*$ generated by $\chi_1, \dots, \chi_j$. This shows the claim. □ □

4.3. **Central extensions.** In this subsection we consider central extensions, as investigated in section 6, from the point of representation theory.

Proposition 29. *Let G be a semi-faithful group and let H be a central subgroup of G with $H \cap [G,G] = \{e\}$. Let H' be a direct factor of $G/[G,G]$ containing the image of H under the embedding $H \hookrightarrow G/[G,G]$ and assume that k contains a primitive root of unity of order $\exp H'$. Then*

$$\operatorname{rdim}_k G - \operatorname{rk} Z(G,k) \leq \operatorname{rdim}_k G/H - \operatorname{rk} Z(G/H,k).$$

Moreover, if $\operatorname{soc} G$ is a central p-subgroup the above inequality is an equality.

Recall that G is semi-faithful (over k) if and only if either $\operatorname{char} k = 0$ or $\operatorname{char} k = p > 0$ and G has no nontrivial normal p-subgroups. We need some auxiliary results:

Lemma 30. *In the situation of the proposition G/H is semi-faithful as well. Moreover there exist characters $\chi_1, \dots, \chi_r$ of G such that $\bigcap_{i=1}^r \ker \chi_i \cap H = \{e\}$, where $r = \operatorname{rk} H$. In particular G has a faithful completely reducible representation of the form $V = V' \oplus k^r$ where V' is a completely reducible representation of G with kernel H and G acts on k^r via $g(x_1, \dots, x_r) = (\chi_1(g)x_1, \dots, \chi_r(g)x_r)$.*

Lemma 31. *In the situation of the proposition, the quotient homomorphism $\pi\colon G \to G/H$ induces isomorphisms $Z(G)/H \simeq Z(G/H)$ and $Z(G,k)/H \simeq Z(G/H,k)$.*

Proof of Lemma 30. We first show that G/H is semi-faithful over k. The case that $\operatorname{char} k = 0$ is trivial, hence assume that k has prime characteristic p. We now make use of the fact that a group is semi-faithful over k if and only if it does not contain any non-trivial normal abelian p-subgroups. Assume that G/H has a normal abelian p-subgroup $P \neq \{e\}$. Then the inverse image B' of P under the natural projection is abelian again, since $[B', B'] \subseteq [G,G] \cap H = \{e\}$. Its p-Sylow subgroup is then a nontrivial normal abelian p-subgroup of G. This contradicts to the assumption that G is semi-faithful over k.

Now let H' be a direct factor of the image of H in $G/[G,G]$ with $\zeta_{\exp H'} \in k$ and let Z denote its complement. Since k contains a primitive root of order $\exp H'$ there exist characters $\tilde{\chi}_1, \dots, \tilde{\chi}_r$ of H' such that $\bigcap_{i=1}^r \ker \tilde{\chi}_i$ intersects trivially with the image of H in H'. Now define χ_i by $\chi_i(g) = \chi_i(\pi_2\pi_1(g))$ where $\pi_1\colon G \to G/[G,G]$ and $\pi_2\colon G/[G,G] \simeq H' \times Z \to H'$ are the obvious projection homomorphisms. By construction $\bigcap_{i=1}^r \ker \chi_i \cap H = \{e\}$. □ □

Remark 5. Actually one can show that the conditions of Proposition 29 are equivalent to the existence of a faithful representation of G of the form given in Lemma 30. The most economical choice for H' is the (unique up to isomorphism) maximal subgroup of $G/[G,G]$ subject to the condition $\operatorname{soc} H' = \operatorname{soc} H$, or in other words, such that for every prime p the p-Sylow-subgroup of H' contains the p-Sylow-subgroup of H and has the same rank.

Proof of Lemma 31. Restricting π to $Z(G)$ and $Z(G,k)$ we get homomorphism $Z(G) \to Z(G/H)$ and $Z(G,k) \to Z(G/H,k)$. It remains to show that the two maps are surjective. The map $Z(G) \to Z(G/H)$ is easily seen to be surjective, because if some $g \in G$ commutes with any other $g' \in G$ up to elements of H, then it is central, because $[G,G] \cap H = \{e\}$. For the second map let $\pi_2\colon G/[G,G] = Z \times H' \to H'$

denote the projection and consider the homomorphism $G \to G/H \times H', g \mapsto (\pi(g), \pi_2(g[G,G]))$, which is injective. If $\pi(g) \in Z(G/H,k)$ then k contains a primitive root of unity of order $\operatorname{ord}(\pi(g))$ as well as a primitive root of unity of order $\exp H'$. Thus k contains a primitive root of unity of order $\operatorname{ord} g$, whence $g \in Z(G,k)$. □ □

Proof of Proposition 29. Using induction on the order of H we may assume that H is cyclic: The case that $|H| = 1$ is clear. If $|H| > 1$ then H contains some cyclic subgroup $H_0 \subsetneq H$. By Lemma 30 G/H_0 is semi-faithful. If H' is a direct factor of $G/[G,G]$ containing H then it contains H_0 as well. Moreover H'/H_0 is a direct factor of $(G/H_0)/[G/H_0, G/H_0]$ and its exponent is no larger than the exponent of H'. Induction yields for the subgroups $H_0 \subseteq G$ and $H/H_0 \subseteq G/H_0$:

$$\operatorname{rdim}_k G - \operatorname{rk} Z(G,k) \le \operatorname{rdim}_k G/H_0 - \operatorname{rk} Z(G/H_0,k)$$
$$\operatorname{rdim}_k G/H_0 - \operatorname{rk} Z(G/H_0,k) \le \operatorname{rdim}_k G/H - \operatorname{rk} Z(G/H,k),$$

with equality if $\operatorname{soc} G$ (and therewith $\operatorname{soc}(G/H)$) is a central p-subgroup. Combining the two lines shows the claim.

We assume now that H is cyclic. Let V be a faithful representation of G/H with $\dim V = \operatorname{rdim}_k G/H$. By Lemma 19 we may assume that V is completely reducible, $V = \bigoplus_{i=1}^n V_i$ for some $n \in \mathbb{N}$ and irreducible representations V_i. We must construct a faithful representation of G of dimension $\dim V + \operatorname{rk} Z(G,k) - \operatorname{rk} Z(G/H,k)$. By (the proof of) Lemma 30 there exists a faithful representation of G of the form $V \oplus k_\chi$ where χ is a character whose restriction to H is faithful.

If $\operatorname{rk} Z(G,k) = \operatorname{rk} Z(G/H,k) + 1$ this does the job. Otherwise $\operatorname{rk} Z(G,k) = \operatorname{rk} Z(G/H,k)$ and we will consider representations $V_{m_1,\dots,m_n} := \bigoplus_{i=1}^n V_i \otimes \chi^{m_i}$ for $m_1, \cdots, m_n \in \mathbb{Z}$. Clearly $V_{m_1,\dots,m_n}$ has the right dimension. We will choose $m_1, \dots, m_n$ such that $V_{m_1,\dots,m_n}$ becomes faithful. In general let g act trivially on $V_{m_1,\dots,m_n}$. This implies that for each i the element g acts like χ^{-m_i} on V_i. In particular the image of g in G/H is an element of $Z(G/H,k)$. Since $Z(G/H,k) \simeq Z(G,k)/H$ under the canonical projection this implies that $g \in Z(G,k)$. Hence $V_{m_1,\dots,m_n}$ is a faithful representation of G if and only if it is faithful restricted to $Z(G,k)$.

The elements of $Z(G,k)$ act through multiplication with characters $\chi_1, \dots, \chi_n$ of $Z(G,k)$ on $V_1, \dots, V_n$. Let $\hat\chi$ denote the restriction of χ to $Z(G,k)$. Then the elements of $Z(G,k)$ act through the characters $\chi_1\hat\chi^{m_1}, \dots, \chi_n\hat\chi^{m_n}$ on the irreducible components of $V_{m_1,\dots,m_n}$. Using (the second part) of the following Lemma 32 we find $m_1, \dots, m_n$ such that $\chi_1\hat\chi^{m_1}, \dots, \chi_n\hat\chi^{m_n}$ generate the whole group $\operatorname{Hom}(Z(G,k), \mathbb{G}_m)$ of characters. Then $V_{m_1,\dots,m_n}$ is faithful restricted to $Z(G,k)$, hence, as previously observed, faithful for G.

Now assume that $C := \operatorname{soc} G$ is a central p-group. It then consist precisely of the central elements of exponent p of G. We want to show $\operatorname{rdim}_k G/H \le \operatorname{rdim}_k G - (\operatorname{rk} Z(G,k) - \operatorname{rk} Z(G/H,k))$. By assumption k contains a primitive root of unity of order $|H|$ and we may assume $H \ne \{e\}$, hence $\zeta_p \in k$. Let $V = \bigoplus_{i=1}^r V_i$ be a faithful representation of G with $\operatorname{rdim}_k G = \dim V$ and each V_i irreducible. There exist characters $\chi_1, \dots, \chi_r \in C^* := \operatorname{Hom}(C, k^*)$ such that $cv_i = \chi_i(c)v_i$ for $c \in C$ and $v_i \in V_i$. Faithfulness of V is equivalent to the statement that $\chi_1, \dots, \chi_r$ generate C^*. In particular $r = \operatorname{rk} Z(G) = \operatorname{rk} C$, since V is minimal. Now as in the first part of the proof let $\chi \in \operatorname{Hom}(G, k^*)$ be a character which is faithful restricted to H. By elementary linear algebra there exists $i \in \{1, \dots, r\}$ such that

$\chi_1, \dots, \chi_{i-1}, \chi|_H, \chi_{i+1}, \dots, \chi_r$ is a basis of C^*. Replacing V_i by k_χ we get a faithful representation of G of minimal dimension which is of the form $V' \oplus k_\chi$. Moreover by multiplying the irreducible components of V' with suitable powers of χ we may assume that H acts trivially on V'. Then the representation $V'' := k_{\chi^{|H|}} \oplus V'$ is a faithful representation of G/H. This establishes the inequality $\operatorname{rdim}_k G/H \leq \operatorname{rdim}_k G - (\operatorname{rk} Z(G) - \operatorname{rk} Z(G/H))$ in case that $\operatorname{rk} Z(G) = \operatorname{rk} Z(G/H)$. In the other case $\operatorname{rk} Z(G) = \operatorname{rk} Z(G/H) + 1$. In that case $\operatorname{soc}(G/H) \simeq C/(H \cap C)$, which is faithfully represented on V', turning V' into a faithful representation of G/H of dimension $\operatorname{rdim}_k G - 1$. This finishes the proof. □ □

Lemma 32. (A) *Let A be an abelian group generated by $a_1, \dots, a_n \in A$. Then if $\operatorname{rk} A < n$ there exist $e_1, \dots, e_n \in \mathbb{Z}$ co-prime such that $\sum_{i=1}^n e_i a_i = 0$.*

(B) *Let A be an abelian group generated by elements $c_1, \dots, c_n, h$. Assume that $\operatorname{rk} A \leq n$. Then there exist $m_1, \dots, m_n \in \mathbb{Z}$ such that $A = \langle c_1 + m_1 h, \dots, c_n + m_n h \rangle$.*

Proof. (A) This follows from the elementary divisor theorem applied to the kernel of the map $\mathbb{Z}^n \twoheadrightarrow A$ sending the i-th basis vector of $\mathbb{Z}^n$ to $a_i \in A$.

(B) First assume that the order of h is of the form p^l where p is a prime and $l \in \mathbb{N}$. Since $\operatorname{rk} A \leq n$ part (A) shows that there exist $e_1, \dots, e_n, e_0 \in \mathbb{Z}$ co-prime such that $\sum_{i=1}^n e_i c_i = e_0 h$. Now if e_0 is not divisible by p we get that $h \in \langle c_1, \dots, c_n \rangle$ and we can set $m_1 = \dots = m_n = 0$. Otherwise there exists $i \in \{1, \dots, n\}$ such that e_i is not divisible by p. Then choose m_i such that $e_i m_i \equiv 1 - e_0 \pmod{p^l}$ and set $m_j = 0$ for $j \neq i$. Then $\sum_{j=1}^n e_j(c_j + m_j h) = (e_0 + e_i m_i)h = h$, hence $h \in \langle c_1 + m_1 h, \dots, c_n + m_n h \rangle$ and it follows that $A = \langle c_1 + m_1 h, \dots, c_n + m_n h \rangle$.

Now if h is arbitrary we decompose it as $h = \sum_{i=1}^s h_i$ where h_i is of order p^{l_i} for some primes $p_1 < \dots < p_s$ and $l_1, \dots, l_s \in \mathbb{N}$ and apply the just proved statement iteratively to $A_j = \langle c_1, \dots, c_n, h_1, \dots, h_j \rangle$ for $j = 1 \dots s$ with generators taken from the previous step plus h_j. This gives elements $m_{i,j}$, $1 \leq i \leq n, 1 \leq j \leq s$ with $A_j = \langle c_1 + \sum_{t=1}^j m_{1,t} h_t, \dots, c_n + \sum_{t=1}^j m_{n,t} h_t \rangle$. We have $A = A_s$. The Chinese remainder theorem now implies the claim.

□ □

Corollary 33. *Let G and A be groups, where G is semi-faithful and A is abelian. Assume that k contains a primitive root of unity of order $\exp A$. Then*

$$\operatorname{rdim} G \times A - \operatorname{rk} Z(G, k) \times A \leq \operatorname{rdim} G - \operatorname{rk} Z(G, k)$$

with equality if $\operatorname{soc} G$ is a central p-subgroup.

Proof. Apply Proposition 29 to the central subgroup $\{e\} \times A \subseteq G \times A$. □ □

5. Relation of covariant and essential dimension

The following theorem generalizes [KLS08, Theorem 3.1], which covers the case $k = \mathbb{C}$.

Theorem 34. *Let G be non-trivial and semi-faithful. Then* $\operatorname{covdim}_k G = \operatorname{edim}_k G$ *if and only if $Z(G, k)$ is non-trivial. Otherwise* $\operatorname{covdim}_k G = \operatorname{edim}_k G + 1$.

Remark 6. The theorem does not hold if $\operatorname{char} k = p$ and G contains a normal p-subgroup. Consider for example an elementary abelian p-group, which has essential dimension 1 by [Le07, Proposition 5], but covariant dimension 2, as the following argument shows: It is enough to consider the case $G = \mathbb{Z}/p\mathbb{Z}$. Let V denote the 2-dimensional representation of G where a generator $g \in G$ acts as $g(s,t) = (s, s+t)$. Suppose that there exists a regular faithful covariant $\varphi\colon \mathbb{A}(V) \to \mathbb{A}(V)$ with $X = \overline{\operatorname{im}\varphi}$ of dimension 1. Then any element g induces an automorphism of order p on the normalization of X, which is isomorphic to $\mathbb{A}^1$. Since in characteristic p no automorphism of $\mathbb{A}^1$ of order p has fixed points we get a contradiction.

The proof of Theorem 34 remains basically the same as in [KLS08, section 3]. We will append it for convenience.

Proof of Theorem 34. Let $Z := Z(G,k)$ and let $V = \bigoplus_{i=1}^n V_i$ be a faithful representation where each V_i is irreducible. The case when Z is trivial follows from Theorem 12, since M_φ cannot be the zero-matrix for any regular multihomogeneous covariant $\varphi\colon \mathbb{A}(V) \to \mathbb{A}(V)$. Thus assume that Z is non-trivial. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal multihomogeneous covariant.

First assume that there exists a row vector $\beta \in \mathbb{Z}^n$ such that all entries of $\alpha := \beta M_\varphi$ are strictly positive. We may assume that φ is of the form $\varphi = \frac{\psi}{f}$ where $f \in k[V]^G$ is multihomogeneous and $\psi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ is a (faithful) regular multihomogeneous covariant. Consider $\tilde{\varphi} = (f^{\alpha_1}\varphi_1, \dots, f^{\alpha_n}\varphi_n)$. It is of the form $\gamma\varphi$ where $\gamma \in \operatorname{Hom}(X(T_V), \mathcal{M}_G(V))$ is of type I relative to φ. Since $\alpha_j > 0$ for all j the covariant $\tilde{\varphi}$ is regular. Lemma 11 implies

$$\operatorname{covdim}_k G \le \dim \tilde{\varphi} \le \dim \varphi = \operatorname{edim}_k G.$$

We reduce to the case above by post-composing with a covariant as in Example 1. Let $g \in Z \setminus \{e\}$ and write $M_\varphi = (m_{ij})$. Since V is faithful the element g acts non-trivially on some V_j. For such j one of the m_{ij}'s must be non-zero. Fix i_0 and j_0 with $m_{i_0 j_0} \neq 0$. Then $\varphi_{j_0} \neq 0$ and we can find a homogeneous $h \in k[W_{j_0}]^G$ of degree $\deg h > 0$ such that $h \circ \varphi_{j_0} \neq 0$. For any $r \in \mathbb{Z}$ consider the covariant

$$\varphi'\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V), \quad v \mapsto h^r(\varphi_{j_0}(v))\varphi(v).$$

Since $h \circ \varphi_{j_0} \neq 0$ and φ is faithful, φ' is faithful, too. Clearly $\dim \varphi' \le \dim \varphi = \operatorname{edim}_k G$. Moreover φ' is multihomogeneous of degree $M_{\varphi'} = (m'_{ij})$ where $m'_{ij} = m_{ij} + r \deg h m_{ij_0}$. For suitable $r \in \mathbb{Z}$ this yields a matrix $M_{\varphi'}$ where all $m'_{i_0 j}$ for $j = 1 \dots n$ are strictly positive. Now for $\beta = e_{i_0}$ the entries of $\alpha = \beta M_\varphi$ are all strictly positive and we are in the case above. □ □

6. The central extension theorem

As announced in the introduction we shall prove a generalization of the central extension theorem.

Theorem 35. *Let G be a semi-faithful group. Let H be a central subgroup of G with $H \cap [G,G] = \{e\}$. Let H' be a direct factor of $G/[G,G]$ containing the image of H under the embedding $H \hookrightarrow G/[G,G]$ and assume that k contains a primitive root of unity of order $\exp H'$. Then*

$$\operatorname{edim}_k G - \operatorname{rk} Z(G,k) = \operatorname{edim}_k G/H - \operatorname{rk} Z(G/H,k).$$

Remark 7. Theorem 35 generalizes the following results about central extensions: [BR97, Theorem 5.3], [Ka06, Theorem 4.5], [KLS08, Corollary 3.7 and Corollary 4.7], as well as [BRV08, Theorem 7.1 and Corollary 7.2] and [BRV07, Lemma 11.2]. Chang's version generalizes the result of Buhler and Reichstein to fields of arbitrary characteristic. A closer look reveals that it covers precisely the case of Theorem 35 when H is cyclic of prime order and maximal amongst cyclic subgroups of $Z(G,k)$. The results of [KLS08] do not have these additional assumptions, but they only work for groups G with $\operatorname{rk} Z(G) \leq 2$ and are formulated for the field of complex numbers. Brosnan, Reichstein and Vistoli's Lemma 11.2 from [BRV07] gives the inequality $\operatorname{edim}_k G \geq \operatorname{edim}_k G/H$. Theorem 7.1 from [BRV08] for fields with $\operatorname{char} k \nmid |G|$ extends [Ka06, Theorem 4.5] in the sense that it does not assume any more that H has prime order, but still it makes the assumption that H is maximal amongst central cyclic subgroups of G. Corollary 7.2 from [BRV08] is restricted to p-groups and it assumes that H is a direct factor of $Z(G)$.

If G is a p-group then Theorem 35 can be deduced from the theorem of Karpenko and Merkurjev about the essential dimension of p-groups and Proposition 29.

Proof of Theorem 35. As in the proof of Proposition 29 we may assume that H is cyclic and there is a faithful representation of G of the form $V \oplus k_\chi$ where χ is faithful on H and $V = \bigoplus_{i=1}^n V_i$ is a completely reducible representation with kernel H. We prove the two inequalities of the equation $\operatorname{edim}_k G - \operatorname{edim}_k G/H = \operatorname{rk} Z(G,k) - \operatorname{rk} Z(G/H,k)$ separately:

"$\leq$": Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal faithful multihomogeneous covariant of G/H. Define a faithful covariant of G via

$$\Phi\colon \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_\chi), \quad (v,t) \mapsto (\varphi(v),t).$$

Clearly Φ is multihomogeneous again of rank $\operatorname{rk} M_\Phi = \operatorname{rk} M_\varphi + 1 = \operatorname{rk} Z(G/H,k) + 1$. Moreover by Theorem 12,

$$\operatorname{edim}_k G \leq \dim \Phi - (\operatorname{rk} M_\Phi - \operatorname{rk} Z(G,k)) = \operatorname{edim}_k G/H - \operatorname{rk} Z(G/H,k) + \operatorname{rk} Z(G,k).$$

"$\geq$": Let $\varphi\colon \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_\chi)$ be a minimal faithful multihomogeneous covariant of G. Let $m := |H|$ and consider the G-equivariant regular map $\pi\colon \mathbb{A}(V \oplus k_\chi) \to \mathbb{A}(V \oplus k_{\chi^m})$ defined by sending $(v,t) \mapsto (v,t^m)$. It is a quotient of $\mathbb{A}(V \oplus k_\chi)$ by the action of H. The composition $\varphi' := \pi \circ \varphi\colon \mathbb{A}(V \oplus k_\chi) \dashrightarrow \mathbb{A}(V \oplus k_{\chi^m})$ is H-invariant, hence we get a commutative diagram:

$$\begin{array}{ccc} \mathbb{A}(V \oplus k_\chi) & \overset{\varphi}{\dashrightarrow} & \mathbb{A}(V \oplus k_\chi) \\ \downarrow{\scriptstyle \pi} & \searrow^{\varphi'} & \downarrow{\scriptstyle \pi} \\ \mathbb{A}(V \oplus k_{\chi^m}) & \overset{\bar{\varphi}}{\dashrightarrow} & \mathbb{A}(V \oplus k_{\chi^m}) \end{array}$$

where $\bar{\varphi}\colon \mathbb{A}(V \oplus k_{\chi^m}) \dashrightarrow \mathbb{A}(V \oplus k_{\chi^m})$ is a faithful G/H-covariant. Since π is finite the rational maps φ, φ' and $\bar{\varphi}$ all have the same dimension $\operatorname{edim}_k G$. Moreover φ' and $\bar{\varphi}$ are multihomogeneous as well. The degree matrix $M_{\varphi'}$ is obtained from M_φ by multiplying its last column by m and from $M_{\bar{\varphi}}$ by multiplying its last row by m. Hence $\operatorname{rk} M_\varphi = \operatorname{rk} M_{\varphi'} = \operatorname{rk} M_{\bar{\varphi}}$. Application of Theorem 12 yields: $\operatorname{edim}_k G/H - \operatorname{rk} Z(G/H,k) \leq \dim \bar{\varphi} - \operatorname{rk} M_{\bar{\varphi}} = \operatorname{edim}_k G - \operatorname{rk} Z(G,k)$.This finishes the proof. □ □

Corollary 36. *Let G and A be groups, where G is semi-faithful and A is abelian. Assume that k contains a primitive root of unity of order* $\exp A$. *Then*

$$\operatorname{edim}_k G \times A - \operatorname{rk} Z(G,k) \times A = \operatorname{edim}_k G - \operatorname{rk} Z(G,k).$$

Proof. Apply Theorem 35 to the central subgroup $\{e\} \times A \subseteq G \times A$. □ □

Example 2. Consider a group G_0 which is generated by a normal subgroup H and an element $g \in G_0 \setminus H$. Let $m := \operatorname{ord}(g)$ and $n := \operatorname{ord}(gH)$ be the orders of g in G and in the quotient G/H. We form the semi-direct product $G := C_m \ltimes H$ by letting a generator c of C_m act on H via conjugation by g. Consider the surjective homomorphism

$$\alpha\colon G = C_m \ltimes H \to G_0 \text{ given by } \alpha(c) = g \text{ and } \alpha(h) = h \text{ for } h \in H.$$

Its kernel is generated by $x := c^n g^{-n}$, hence cyclic of order $r := m/n$. The elements c and g^n commute in G and x lies in the center of G, since $[x,c] = e$ and $[x,h] = (c^n(g^{-n}hg^n)c^{-n})h^{-1} = (g^n(g^{-n}hg^n)g^{-n})h^{-1} = e$ for $h \in H$. We obtain a central extension

$$1 \to C_r \to G \to G_0 \to 1.$$

The intersection $[G,G] \cap \langle x \rangle$ is trivial, since $[G,G] \subseteq H$. Now let π be the set of prime divisors of the order of the abelian socle of $G = C_m \ltimes H$ and assume $\operatorname{char} k \notin \pi$. Then

$$\operatorname{edim}_k C_m \ltimes H = \operatorname{edim}_k G_0 + \operatorname{rk} Z(C_m \ltimes H, k) - \operatorname{rk} Z(G_0, k).$$

Another application of the central extension theorem is the following:

Corollary 37. *Let G be a semi-faithful group with faithful completely reducible representation V. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal faithful multihomogeneous covariant. Assume that k contains a primitive root of unity of order p for some prime p. Then the rational map $\pi_V \circ \varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{P}(V)$ has exactly dimension* $\dim \varphi - \operatorname{rk} Z(G,k)$.

Proof. The inequality $\dim \pi_V \circ \varphi \le \dim \varphi - \operatorname{rk} Z(G,k)$ was already shown previously. We use saturation to prove the reversed inequality. We may assume that the rank of $Z(G,k)$ equals the rank of its p-Sylow subgroup. By Proposition 25 V admits a faithful representation of $\tilde{G} := G \times C_p^{n-r}$ where $n = \dim T_V$ and $r = \operatorname{rk} Z(G,k) = \operatorname{rk} M_\varphi$.

Corollary 9 implies the existence of $\gamma \in \operatorname{Hom}(X(T_V), \mathcal{M}_G(V))$ such that $\gamma\varphi$ is D-equivariant for $D = \operatorname{Id}_{T_V}$. This turns $\tilde{\varphi} := \gamma\varphi$ into a faithful (multihomogeneous) covariant for $\tilde{G}$. Corollary 36 shows that $\dim \tilde{\varphi} \ge \operatorname{edim}_k \tilde{G} = \operatorname{edim}_k G + (n-r)$. Since $\pi_V \circ \tilde{\varphi} = \pi_V \circ \varphi$ we get $\dim \pi_V \circ \varphi = \dim \pi_V \circ \tilde{\varphi} \ge \dim \tilde{\varphi} - n \ge \dim \varphi - r$, showing the claim. □ □

7. Subgroups and direct products

Proposition 38. *Let $H \subseteq G$ be a subgroup. Assume that G has a completely reducible faithful representation which remains completely reducible when restricted to H. Then*

$$\operatorname{edim}_k G - \operatorname{rk} Z(G,k) \ge \operatorname{edim}_k H - \operatorname{rk} Z(H,k).$$

Proof. Let $V = \bigoplus_{i=1}^m V_i$ be a faithful representation of G with each V_i irreducible and completely reducible as a representation of H and let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a minimal faithful covariant which is multihomogeneous. By Theorem 12 $\operatorname{rk} M_\varphi = \operatorname{rk} Z(G,k)$. Now consider φ as covariant for H. By Proposition 16 the rank doesn't go down replacing φ by a multihomogenization $H_\lambda(\varphi)$ with respect to a refinement into irreducible representations for H. Hence again by Theorem 12 $\operatorname{edim}_k H - \operatorname{rk} Z(H,k) \leq \dim H_\lambda(\varphi) - \operatorname{rk} M_{H_\lambda(\varphi)} \leq \dim \varphi - \operatorname{rk} M_\varphi = \operatorname{edim}_k G - \operatorname{rk} Z(G,k)$. □ □

Remark 8. There exist pairs (H,G) of a group G with subgroup H such that both H and G are semi-faithful over k, but none of the completely reducible faithful representations of G restricts to a completely reducible representation of H. We found some examples using the computer algebra system [MAGMA], the smallest (in terms of the order of G) is a pair of the form $H = S_3$, $G = C_2 \ltimes (C_3 \ltimes (C_3 \times C_3))$ in characteristic 2. Also there are examples in order 72 with $G = Q_8 \ltimes (C_3 \times C_3)$ or $G = C_8 \ltimes (C_3 \times C_3)$.

Proposition 39. *Let G_1 and G_2 be semi-faithful groups. Then*

$$\operatorname{edim}_k G_1 \times G_2 - \operatorname{rk} Z(G_1 \times G_2, k) \leq \operatorname{edim}_k G_1 - \operatorname{rk} Z(G_1, k) + \operatorname{edim}_k G_2 - \operatorname{rk} Z(G_2, k).$$

Proof. Let $V = \bigoplus_{i=1}^m V_i$ and $W = \bigoplus_{j=1}^n W_j$ be faithful representations of G_1 and G_2, respectively, where each V_i and W_j is irreducible. Let $\varphi_1\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ and $\varphi_2\colon \mathbb{A}(W) \dashrightarrow \mathbb{A}(W)$ be minimal faithful multihomogeneous covariants for G_1 and G_2. Then $\operatorname{rk} M_{\varphi_1} = \operatorname{rk} Z(G_1,k)$ and $\operatorname{rk} M_{\varphi_2} = \operatorname{rk} Z(G_2,k)$ by Theorem 12. The covariant $\varphi_1 \times \varphi_2\colon \mathbb{A}(V \oplus W) \dashrightarrow \mathbb{A}(V \oplus W)$ for $G_1 \times G_2$ is again faithful and multihomogeneous with $\operatorname{rk} M_\varphi = \operatorname{rk} M_{\varphi_1} + \operatorname{rk} M_{\varphi_2} = \operatorname{rk} Z(G_1,k) + \operatorname{rk} Z(G_2,k)$. Thus, by Theorem 12,

$$\begin{aligned}\operatorname{edim}_k G_1 \times G_2 - \operatorname{rk} Z(G_1 \times G_2, k) &\leq \dim \varphi - \operatorname{rk} M_\varphi \\ &= \dim \varphi_1 + \dim \varphi_2 - \operatorname{rk} Z(G_1,k) - \operatorname{rk} Z(G_2,k).\end{aligned}$$

Since $\dim \varphi_1 = \operatorname{edim}_k G_1$ and $\dim \varphi_2 = \operatorname{edim}_k G_2$ this implies the claim. □ □

Remark 9. We do not know of an example where the inequality in Proposition 39 is strict.

8. Twisting by torsors

Let $V = \bigoplus_{i=1}^m V_i$ be a faithful representation of G where each V_i is irreducible and let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ be a multihomogeneous covariant of G with $\varphi_j \neq 0$ for all j. We denote by $\mathbb{P}(V) := \mathbb{P}(V_1) \times \ldots \times \mathbb{P}(V_m)$ the product of the projective spaces. It is the quotient of a dense open subset of $\mathbb{A}(V)$ by the action of T_V. We write $\pi_V\colon \mathbb{A}(V) \dashrightarrow \mathbb{P}(V)$ for the corresponding rational quotient map. Since φ is multihomogeneous there exists a unique rational map $\psi\colon \mathbb{P}(V) \dashrightarrow \mathbb{P}(V)$ making the diagram

$$\begin{array}{ccc} \mathbb{A}(V) & \overset{\varphi}{\dashrightarrow} & \mathbb{A}(V) \\ \downarrow \pi_V & & \downarrow \pi_V \\ \mathbb{P}(V) & \overset{\psi}{\dashrightarrow} & \mathbb{P}(V) \end{array}$$

commute. Let $Z := Z(G,k)$, which acts trivially on $\mathbb{P}(V)$ and let $C \subseteq Z$ be any subgroup. We view ψ as an $H := G/C$-equivariant rational map. We will twist the map

ψ (after scalar extension) by some H-torsor to get a rational map between products of Severy-Brauer varieties. We summarize the construction and basic properties of the twist construction, cf. [Fl08, section 2]:

Let K be a field and H be a finite group. A *(right-) H-torsor* (over K) is a non-empty not necessarily irreducible K-variety E equipped with a right action of H such that H acts freely and transitively on $E(K_{\rm sep})$. The isomorphism classes of H-torsors (over K) correspond bijectively to the elements of the Galois cohomology set $H^1(K,H)$, where an isomorphism class of an H-torsor E corresponds to the class of the cocycle $\alpha=(\alpha_\gamma)_{\gamma\in\Gamma_K}$ defined by $\gamma x = x\alpha_\gamma$, where x is any fixed element of E and $\Gamma_K=\mathrm{End}_K(K_{\rm sep})$ is the absolute Galois-group of K. Every H-torsor is of the form $\operatorname{Spec} L$ where L/K is a Galois H-algebra.

Let X be a quasi-projective H-variety over K. Let H act on the product $E\times X$ by $h(e,x)=(eh^{-1},hx)$. Then the quotient $(E\times X)/H$ exists in the category of K-varieties and will be denoted by ${}^EX$. It is called the *twist of the H-variety X by the torsor E*.

If X and Y are quasi-projective H-varieties and $\psi\colon X\dashrightarrow Y$ is a rational map, there exists a canonical rational map ${}^E\psi\colon {}^EX\dashrightarrow {}^EY$. Moreover if Z is another quasi-projective variety and $\psi_1\colon X\dashrightarrow Y$ and $\psi_2\colon Y\dashrightarrow Z$ are composable, then ${}^E\psi_1\colon {}^EX\dashrightarrow {}^EY$ and ${}^E\psi_2\colon {}^EY\dashrightarrow {}^EZ$ are composable as well with composition ${}^E(\psi_2\circ\psi_1)$.

Let A be a central simple K-algebra on which H acts on the left by algebra-homomorphisms. Let E be a H-torsor corresponding to a Galois H-algebra L/K. The *twist of A by the torsor E*, denoted by ${}^EA$ is defined to be the subalgebra of H-invariants of $A\otimes_K L$ where H acts via $h(a\otimes l)=ha\otimes hl$.

If $E\simeq H$ is the trivial H-torsor then the twist ${}^EX$ (resp. ${}^EA$) is isomorphic to X (resp. A). The varieties X and ${}^EX$ (resp. the algebras A and ${}^EA$) become isomorphic over a splitting field K'/K of E (i.e. over a field where E has a K'-rational point). Let U be a K-vector space of dimension n. The algebra $\mathrm{End}_K(U)$ carries an action from $\mathrm{PGL}(U)$ via conjugation. Isomorphism classes of central simple K-algebras of degree n correspond bijectively to the elements of $H^1(K,\mathrm{PGL}(U))$, via the following assignment: For $T\in H^1(K,\mathrm{PGL}(U))$, represented by a cocycle $\alpha=(\alpha_\gamma)_{\gamma\in\Gamma_K}$, the corresponding central simple algebra is defined to be the sub-algebra of invariants of $\mathrm{End}(U)\otimes_K K_{\rm sep}$ under the action of Γ_K twisted through α, defined by $\gamma\cdot_\alpha(\varphi\otimes\lambda)=(\alpha_\gamma\varphi)\otimes(\gamma\lambda)$ for $\varphi\in\mathrm{End}(U)$ and $\lambda\in K_{\rm sep}$.

The three different notions of twisting are related as follows:

Lemma 40. *Let U be a K-vector space of dimension n. The group $\mathrm{PGL}(U)$ acts on $\mathbb{P}(U)$ from the right in the obvious way and on $\mathrm{End}(U)$ via conjugation from the left. Let $\beta\colon H\to\mathrm{PGL}(U)$ be a homomorphism and let E be a H-torsor over K. Let H act on $\mathbb{P}(U)$ and on $\mathrm{End}(U)$ via the homomorphism β. Then ${}^E\mathbb{P}(U)\simeq \mathrm{SB}(A)$ where $A:={}^E\mathrm{End}(U)$. Moreover A is isomorphic to the central simple algebra corresponding to the image of E under the map $H^1(K,H)\xrightarrow{\beta_*}H^1(K,\mathrm{PGL}(U))$.*

Proof. The first part is [Fl08, Lemma 3.1]. For the second part, let $E=\mathrm{Spec}(L)$ for some Galois H-algebra L and fix $\iota\in\mathrm{Hom}(L,K_{\rm sep})=E(K_{\rm sep})$. Then the image of E in $H^1(K,\mathrm{PGL}(U))$ is represented by the cocycle $\alpha=(\beta(h_\gamma))_{\gamma\in\Gamma_K}$ where $h_\gamma\in H$ is such that ${}^\gamma\iota=\iota h_\gamma$. In other words $\gamma(\iota(\ell))=(\iota h_\gamma)(\ell)=\iota(h_\gamma\ell)$ for all $\ell\in L$. Recall that $A={}^E\mathrm{End}(U)$ is the sub-algebra of H-invariants of $\mathrm{End}(U)\otimes L$ and the twist B of $\mathrm{End}(U)$ by the cocycle α is the sub-algebra of Γ_K invariants of $\mathrm{End}(U)\otimes K_{\rm sep}$

under the action twisted by the cocycle α. Consider the homomorphism of K-algebras $\varepsilon := \mathrm{Id} \otimes \iota \colon \mathrm{End}(U) \otimes L \to \mathrm{End}(U) \otimes K_{\mathrm{sep}}$. It is equivariant in the sense that $\varepsilon(h_\gamma x) = \gamma \cdot_\alpha \varepsilon(x)$ for $x \in \mathrm{End}(U) \otimes L$ and $\gamma \in \Gamma_K$. To see this, we may check it for $x = \varphi \otimes \ell$ where $\varphi \in \mathrm{End}(U)$ and $\ell \in L$. Then $\varepsilon(h_\gamma x) = h_\gamma \varphi \otimes \iota(h_\gamma \ell)$ and $\gamma \cdot_\alpha \varepsilon(x) = \gamma \cdot_\alpha (\varphi \otimes \iota(\ell)) = \beta(h_\gamma)\varphi \otimes \gamma(\iota(\ell)) = h_\gamma \varphi \otimes \iota(h_\gamma \ell)$. This shows that $\varepsilon(A) \subseteq B$. Since A is simple, the homomorphism ε maps A injectively into B. Counting dimensions yields $\varepsilon(A) = B$. Hence ε establishes an isomorphism of K-algebras between A and B, showing the claim. □ □

We will now apply the twist construction to our particular situation. Let K/k be a field extension and E be an H-torsor over K. Extending scalars to K we may twist the map ψ_K with E and get a rational map ${}^E\psi_K \colon {}^E\mathbb{P}(V_K) \dashrightarrow {}^E\mathbb{P}(V_K)$.

Lemma 41. *${}^E\mathbb{P}(V_K) \simeq \prod_{i=1}^m \mathrm{SB}(A_i)$, where A_i is the twist of $\mathrm{End}_K(V_i \otimes K)$ by the H-torsor E and $\mathrm{End}_K(V_i \otimes K)$ carries the conjugation action induced from G. Moreover the class of A_i in $\mathrm{Br}(K)$ coincides with the image $\beta^E(\chi)$ of E under the map*

$$H^1(K, H) \to H^2(K, C) \xrightarrow{\chi_*} H^2(K, \mathbb{G}_m) = \mathrm{Br}(K)$$

where $\chi \in C^*$ is the character defined by $gv = \chi(g)v$ for $g \in C$ and $v \in V_i$.

Proof. The first claim follows from Lemma 40. For the second claim (cf. [KM08, Lemma 4.3]) consider the commutative diagram

$$\begin{array}{ccc} H^1(K, H) & \longrightarrow & H^2(K, C) \\ \downarrow & & \downarrow{\scriptstyle (\chi_i)_*} \\ H^1(K, \mathrm{PGL}(V_i \otimes K)) & \longrightarrow & H^2(K, \mathbb{G}_m) \end{array}$$

arising from the following commutative diagram with exact rows:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & C & \longrightarrow & G & \longrightarrow & H & \longrightarrow & 1 \\ & & \downarrow{\scriptstyle \chi_i} & & \downarrow{\scriptstyle \rho_{V_i \otimes K}} & & \downarrow & & \\ 1 & \longrightarrow & \mathbb{G}_m & \longrightarrow & \mathrm{GL}(V_i \otimes K) & \longrightarrow & \mathrm{PGL}(V_i \otimes K) & \longrightarrow & 1. \end{array}$$

This shows that the image $\beta^E(\chi_i)$ of a torsor E over K in $H^2(K, \mathbb{G}_m)$ coincides with the Brauer-class of the central simple algebra corresponding to the image of E in $H^1(K, \mathrm{PGL}(V_i \otimes K))$. By Lemma 40 this is precisely the twist of $\mathrm{End}(V_K)$ by the H-torsor E. □ □

Definition 12. Let X and Y be smooth projective varieties. The number $e(X)$ is defined as the least dimension of the closure of the image of a rational map $X \dashrightarrow X$.

Let $\mathcal{C}$ be a class of field extensions of some field K. A generic field of $\mathcal{C}$ is a field $E \in \mathcal{C}$ such that for every $L \in \mathcal{C}$ there exists a k-place $E \rightsquigarrow L$. The canonical dimension of $\mathcal{C}$ is the least transcendence degree over K of a generic field of $\mathcal{C}$, denoted by $\mathrm{cd}(\mathcal{C})$ (possibly infinite).

If X is a K-variety or if $D \subseteq \mathrm{Br}(K)$ is a subgroup, the canonical dimension of X (resp. D) is defined as the canonical dimension of the class of splitting fields of X (resp. D), i.e. the class of field extensions L/K, for which $X(L) \neq \emptyset$ (resp. for

which D lies in the kernel of the homomorphism $\mathrm{Br}(K) \to \mathrm{Br}(L)$). It is denoted by $\mathrm{cd}(X)$ (resp. $\mathrm{cd}(D)$).

Lemma 42 ([KM06, Corollary 4.6])**.** *Let X be a smooth projective K-variety. Then $e(X) = \mathrm{cd}(X)$.*

We only need the inequality $e(X) \geq \mathrm{cd}(X)$ which is established as follows: Let $\psi\colon X \dashrightarrow X$ be a rational map with $\dim \psi = e(X)$ and let Y be the closure of the image of ψ. One can show that $K(Y)$ is a generic splitting field for X. Hence $\mathrm{cd}(X) \leq \mathrm{tdeg}_K K(Y) = \dim \psi = e(X)$.

Lemma 43.

$$\mathrm{edim}_k G - \mathrm{rk}\, Z(G,k) \geq e\left({}^E\mathbb{P}(V_K)\right) = \mathrm{cd}\left({}^E\mathbb{P}(V_K)\right) = \mathrm{cd}(\mathrm{im}\,\beta^E)$$

Proof. Let $\varphi\colon \mathbb{A}(V) \dashrightarrow \mathbb{A}(V)$ and $\psi\colon \mathbb{P}(V) \dashrightarrow \mathbb{P}(V)$ be as in the beginning of this section and assume that φ is minimal, i.e. $\dim \varphi = \mathrm{edim}_k G$. By functoriality we have $\dim {}^E\psi_K \leq \dim \psi_K$. Hence

$$e\left({}^E\mathbb{P}(V_K)\right) \leq \dim {}^E\psi_K \leq \dim \psi_K = \dim \psi.$$

We now show that $\dim \psi \leq \dim \varphi - \mathrm{rk}\, Z(G,k)$. Let $X := \overline{\mathrm{im}\,\varphi} \subseteq \mathbb{A}(V)$. The fibers of $\pi_V|_X\colon X \to \mathbb{P}(V)$ are stable under the torus $D_\varphi(T_V) \subseteq T_V$. The dimension of $D_\varphi(T_V)$ is greater or equal to $\mathrm{rk}\, Z(G,k)$, since it contains the image of $Z(G,k)$ under $G \hookrightarrow \mathrm{GL}(V)$. Moreover $D_\varphi(T_V)$ acts generically freely on X. Hence the claim follows by the fiber dimension theorem. Lemma 42 implies $e\left({}^E\mathbb{P}(V_K)\right) = \mathrm{cd}\left({}^E\mathbb{P}(V_K)\right)$. The equality $\mathrm{cd}\left({}^E\mathbb{P}(V_K)\right) = \mathrm{cd}\,\mathrm{im}\,\beta^E$ follows easily by Lemma 41, since it shows that the class of splitting fields of the variety ${}^E\mathbb{P}(V_K)$ is identical to the class of common splitting fields of $\beta^E(\chi_1), \ldots, \beta^E(\chi_m)$. Since V is faithful restricted to C the characters $\chi_1, \ldots, \chi_m$ generate C^*. Hence the splitting fields of ${}^E\mathbb{P}(V_K)$ are precisely the splitting fields of the image of β^E in $\mathrm{Br}(K)$. □ □

Remark 10. Lemma 43 substitutes one part of the proof of the Theorem of Karpenko and Merkurjev about the essential dimension of a p-group G when k contains a primitive p-th root of unity, saying that $\mathrm{edim}_k G = \mathrm{rdim}_k G$. They show in that case that $\mathrm{edim}_k G \geq \mathrm{edim}[E/G] = \mathrm{cd}(\mathrm{im}\,\beta^E) + \mathrm{rk}\, Z(G)$ where E is a generic G/C-torsor, $C := \mathrm{soc}(Z(G))$ and $[E/G]$ is the corresponding quotient stack, see [KM08, Theorem 4.2 and Theorem 3.1]. Our Lemma is more general because C does not need to be a p-group. Probably one could also use the stack theoretic approach to show the result of Lemma 43, but using multihomogeneous covariants seems more elementary.

Remark 11 (The choice of the subgroups $C \subseteq Z(G,k)$). Karpenko and Merkurjev work with the subgroup of elements of exponent p in $Z(G,k)$. In their setting G is a p-group and $\zeta_p \in k$, so C is the smallest subgroup of $Z(G)$ with the same rank as $Z(G)$. In general the best lower bound is obtained with the maximal choice, i.e. with the subgroup $C = Z(G,k)$. This is seen as follows: Set $Z = Z(G,k)$. For a G/C-torsor E' over K let E denote its image under $H^1(K, G/C) \to H^1(K, G/Z)$. Then for any $\chi \in Z^*$ we have a commutative diagram:

$$\begin{array}{ccccccc}
H^1(K,G/C) & \longrightarrow & H^2(K,C) & \xrightarrow{(\chi|_C)_*} & H^2(K,\mathbb{G}_m) & \longrightarrow & \mathrm{Br}(K) \\
\downarrow & & \downarrow & & \| & & \| \\
H^1(K,G/Z) & \longrightarrow & H^2(K,Z) & \xrightarrow{\chi_*} & H^2(K,\mathbb{G}_m) & \longrightarrow & \mathrm{Br}(K)
\end{array}$$

Since every element of C^* is the restriction of some character $\chi \in Z^*$ this shows that $\operatorname{im}(\beta^E) = \operatorname{im}(\beta^{E'})$, hence their canonical dimensions coincide.

In general we don't know whether the choice of the subgroup of elements of exponent p in $Z(G,k)$ gives the same lower bound.

We quote two key results from [KM08]:

Theorem 44 ([KM08, Theorem 2.1 and Remark 2.9])**.** *Let p be a prime, K be a field and $D \subseteq \operatorname{Br}(K)$ be a finite p-subgroup of rank $r \in \mathbb{N}$. Then $\operatorname{cd} D = \min\{\sum_{i=1}^{r}(\operatorname{Ind} a_i - 1)\}$ taken over all generating sets $a_1, \dots, a_r$ of D. Moreover if D is of exponent p then the minimum is attained for every minimal basis $a_1, \dots, a_r$ of D for the function $d \mapsto \operatorname{Ind} d$ on D.*

Theorem 45 ([KM08, Theorem 4.4 and Remark 4.5])**.** *Let $1 \to C \to G \to H \to 1$ be an exact sequence of algebraic groups over some field k with C central and diagonalizable. Then there exists a generic H-torsor E over some field extension K/k such that for all $\chi \in C^*$:*

$$\operatorname{Ind} \beta^E(\chi) = \gcd\{\dim V \mid V \in \operatorname{rep}^{(\chi)}(G)\}.$$

The following corollary works for a slightly larger class of groups than p-groups. It becomes [KM08, Theorem 4.1] under the observation that all irreducible representations of p-groups have p-primary dimension when $\zeta_p \in k$.

Corollary 46 (cf. [KM08, Theorem 4.1])**.** *Let G be an arbitrary group whose socle C is a central p-subgroup for some prime p and let k be a field containing a primitive p-th root of unity. Assume that for all $\chi \in C^*$ the equality*

$$\gcd\{\dim V \mid V \in \operatorname{rep}^{(\chi)}(G)\} = \min\{\dim V \mid V \in \operatorname{rep}^{(\chi)}(G)\}$$

holds. Then $\operatorname{edim}_k G = \operatorname{rdim}_k G$.

Proof. The inequality $\operatorname{edim}_k G \leq \operatorname{rdim}_k G$ is clear. By the assumption on k we have $\operatorname{rk} C = \operatorname{rk} Z(G,k) = \operatorname{rk} Z(G)$. Hence, by Lemma 43, it suffices to show $\operatorname{cd}(\operatorname{im}\beta^E) = \operatorname{rdim}_k G - \operatorname{rk} C$ for a generic $H := G/C$-torsor E over a field extension K of k.

By Theorem 44 there exists a basis $a_1, \dots, a_s$ of $\operatorname{im}\beta^E$ such that $\operatorname{cd}(\operatorname{im}\beta^E) = \sum_{i=1}^{s}(\operatorname{Ind} a_i - 1)$. Choose a basis $\chi_1, \dots, \chi_r$ of C^* such that $a_i = \beta^E(\chi_i)$ for $i = 1, \dots, s$ and $\beta^E(\chi_i) = 1$ for $i > s$ and choose $V_i \in \operatorname{rep}^{(\chi_i)}(G)$ of minimal dimension. By assumption $\dim V_i = \gcd\left\{\dim V \mid V \in \operatorname{rep}^{(\chi_i)}(G)\right\}$, which is equal to the index of $\beta^E(\chi_i)$ for the H-torsor of Theorem 45.

Set $V = V_1 \oplus \cdots \oplus V_r$. This is a faithful representation since every normal subgroup of G intersects $C = \operatorname{soc} G$ non-trivially. Then $\operatorname{cd}(\operatorname{im}\beta^E) = \sum_{i=1}^{s}(\operatorname{Ind} a_i - 1) = \sum_{i=1}^{r} \operatorname{Ind}\beta^E(\chi_i) - \operatorname{rk} C = \sum_{i=1}^{r} \dim V_i - \operatorname{rk} C = \dim V - \operatorname{rk} C \geq \operatorname{rdim}_k G - \operatorname{rk} C$. The claim follows. □ □

The following was conjectured in case of cyclic subgroups of the Brauer group and proved (over fields of characteristic 0) for cyclic groups of order 6 in [CKM07].

Conjecture 47. *Let $D \subseteq \operatorname{Br}(K)$ be a finite subgroup. Then*

$$\operatorname{cd} D = \sum_p \operatorname{cd} D(p),$$

where $D(p)$ denotes the p-Sylow subgroup of D.

Remark 12. Brosnan, Reichstein and Vistoli asked the following question in [BRV07, section 7]: "Let X and Y be smooth projective varieties over a field K. Assume that there are no rational functions $X \dashrightarrow Y$ or $Y \dashrightarrow X$. Then is it true that $e(X \times Y) = e(X) + e(Y)$?" It remains true in our case that "a positive answer to this question would imply the conjecture above".

Corollary of Conjecture 48. *Let G be a group whose socle $C := \operatorname{soc} G$ is central and let k be a field containing a primitive p-th root of unity for every prime p dividing $|C|$. Assume that for all $\chi \in C^*$ of prime order $\min \dim W = \gcd \dim W$ taken on both sides over all $W \in \operatorname{rep}^{(\chi)}(G)$. Then*

$$\operatorname{edim}_k G = \dim V - \sum_p \operatorname{rk} C(p) + \operatorname{rk} C,$$

where $V = \bigoplus V_p$ is a faithful representation of G, the direct sum being taken over all primes p dividing $|C|$, and V_p is of minimal dimension amongst representations of G whose restriction to $C(p)$ is faithful.

Example 3. Using the computer algebra systems [MAGMA] and [GAP] (and [SAGE] to combine the two) we found several examples of non-nilpotent groups for which [CKM07, Theorem 1.3] applies when k is a field containing $\mathbb{Q}(\zeta_3)$. These are groups (of order 432) with $\operatorname{soc} G = Z(G) \simeq C_6$ whose Sylow 2- and 3-subgroup have essential dimension 2 and 3, respectively. Corollary 48 gives for their essential dimension $\operatorname{edim}_k G = (2+3) - 2 + 1 = 4$.

Proof. "$\leq$": Consider the multihomogeneous covariant $\operatorname{Id}\colon \mathbb{A}(V) \to \mathbb{A}(V)$. Theorem 12 implies $\operatorname{edim}_k G \leq \dim \operatorname{Id} - (\operatorname{rk} M_{\operatorname{Id}} - \operatorname{rk} Z(G,k)) = \dim V - \sum_p \operatorname{rk} C(p) + \operatorname{rk} C$.

"$\geq$": Choose a generic G/C-torsor E. Then $\operatorname{edim}_k G \geq \operatorname{cd}(\operatorname{im} \beta^E) + \operatorname{rk} C$, by Lemma 43. The p-Sylow subgroup of the image of the abelian group $C = \bigoplus_p C(p)$ equals $\beta^E(C(p))$. Conjecture 47 implies that $\operatorname{cd} \operatorname{im} \beta^E = \sum_p \operatorname{cd} \beta^E(C(p))$, which can be computed with the help of Theorems 44 and 45. Similarly as in the proof of Corollary 46 we get the claim, using the replacement of gcd by min. □ □

Example 4. Let G be nilpotent, i.e. the direct product of its Sylow subgroups $G(p)$, p prime. Assume that k contains a primitive p-th root of unity for every prime p dividing $|G|$. Then Conjecture 47 and its corollary imply

$$\operatorname{edim}_k G = \sum_p (\operatorname{rdim}_k G(p) - \operatorname{rk} C(p)) + \operatorname{rk} C.$$

9. Normal elementary p-subgroups

Suppose that we are in the case of a non-semi-faithful group G. Recall that this happens precisely when $\operatorname{char} k = p > 0$ and G contains a nontrivial normal p-subgroup A. Replacing A by the elements of $Z(A)$ of exponent p (which is again normal in G) we may assume that A is p-elementary. In particular $\operatorname{edim}_k A = 1$ by [Le07, Proposition 5]. We would like to relate $\operatorname{edim}_k G$ and $\operatorname{edim}_k G/A$ and use this iteratively to pass to the semi-faithful case.

Merkurjev's description of essential dimension as the essential dimension of the Galois cohomology functor $H^1(\_, G)$ from the category of field extensions of k to the category of sets (see [BF03]) gives the following:

Proposition 49. *If A is an elementary p-group contained in the center of G and if* $\operatorname{char} k = p$ *then*

$$(*) \qquad \operatorname{edim}_k G/A \leq \operatorname{edim}_k G \leq \operatorname{edim}_k G/A + 1.$$

Proof. Since A is central there is the following exact sequence in Galois cohomology:

$$1 \to H^1(\_, A) \to H^1(\_, G) \to H^1(\_, G/A) \to H^2(\_, A) = 1.$$

Thus $H^1(\_, G) \to H^1(\_, G/A)$ is a surjection of functors. In particular $\operatorname{edim}_k G/A \leq \operatorname{edim}_k G$ by [BF03, Lemma 1.9].

We have an action of $H^1(\_, A)$ on $H^1(\_, G)$ as follows: Let K/k be a field extension and let $[\alpha] \in H^1(K, A)$ and $[\beta] \in H^1(K, G)$ and set $[\alpha] \cdot [\beta] := [\alpha\beta] \in H^1(K, G)$. Since A is a central $\alpha\beta$ satisfies the cocyle condition and its class in $H^1(K, G)$ does not depend on the choice of α and β. Moreover it is well known that two elements of $H^1(K, G)$ have the same image in $H^1(K, G/A)$ if and only if one is transformed from the other by an element of $H^1(K, A)$, see [Se64]. Thus we have a transitive action on the fibers of $H^1(K, G) \twoheadrightarrow H^1(K, G/A)$, and this action is natural in K. That means we have a fibration of functors

$$H^1(\_, A) \rightsquigarrow H^1(\_, G) \twoheadrightarrow H^1(\_, G/A).$$

Now [BF03, Proposition 1.13] yields $\operatorname{edim}_k G \leq \operatorname{edim}_k G/A + \operatorname{edim}_k A = \operatorname{edim}_k G/A + 1$. □ □

Remark 13. If G is a p-group and A is a (not necessarily central) elementary abelian p-subgroup contained in the Frattini subgroup of G then [Le04] gives the relations $(*)$ as well.

Example 5. Let G denote the perfect group of order $8! = 40320$ which is a central extension of A_8 by C_2. The socle of this group $\operatorname{soc} G = C_2$ is central.
Claim: $\operatorname{edim}_k G = 8$ if $\operatorname{char} k \neq 2$ and $\operatorname{edim}_k G \in \{2, 3, 4\}$ if $\operatorname{char} k = 2$.

Proof. First consider the case when $\operatorname{char} k \neq 2$. There exists a faithful irreducible representation of G of degree 8 with entries in $\mu_2(k) \simeq C_2$. This implies in particular that $\operatorname{edim}_k G \leq 8$. Moreover one may check using a Computer algebra system like [MAGMA] or [GAP] that the degree of every faithful irreducible representation of G is a multiple of 8. The faithful irreducible representations of G are precisely the elements of $\operatorname{rep}^{(\chi)}(G)$ where χ is the non-trivial character of $\operatorname{soc} G = C_2$. Hence the claim follows with Corollary 46.

Now consider the case of $\operatorname{char} k = 2$. Proposition 49 implies that $\operatorname{edim}_k A_8 \leq \operatorname{edim}_k G \leq \operatorname{edim}_k A_8 + 1$. The essential dimension of $A_8 \simeq \mathrm{GL}_4(\mathbb{F}_2)$ is either 2 or 3, see [Ka06, Lemma 5.5 and Theorem 5.6], and the claim follows. □ □

Acknowledgments

I am grateful to my PhD adviser Hanspeter Kraft for many fruitful discussions about covariant and essential dimension and the content of this paper.

References

[BH08] B. Bekka, P. de la Harpe, *Irreducibly represented groups*, `arXiv:math/0611814v2`.
[BR97] J. Buhler, Z. Reichstein, *On the Essential Dimension of a Finite Group* Compositio Math., **106** (1997), 159–179.
[BRV07] P. Brosnan, Z. Reichstein, A. Vistoli, *Essential dimension and Algebraic stacks*, `http://www.math.ubc.ca/~reichst/pub.html`, 2007.

[BRV08] P. Brosnan, Z. Reichstein, A. Vistoli *Essential dimension and Algebraic stacks I*, Linear Algebraic Groups and Related Structures Preprint Server, `http://www.math.uni-bielefeld.de/LAG/man/275.pdf`, 2008.

[CKM07] J.-L. Colliot-Thélène, N. Karpenko, A. Merkurjev, *Rational surfaces and canonical dimension of* PGL_6.

[BF03] G. Berhuy, G. Favi *Essential Dimension: a Functorial Point of View (after A. Merkurjev)* Documenta Mathematica **8** (2003), 279–330.

[Fl08] M. Florence *On the essential dimension of cyclic p-groups*, Invent. Math. **171** (2008), 175-189.

[Ga54] W. Gaschütz *Endliche Gruppen mit treuen absolut-irreduziblen Darstellungen*. Math. Nachr. **12** (1954) 253-255.

[GAP] M. Schönert et al. GAP Groups, Algorithms, and Programming. Lehrstuhl D für Mathematik, Rheinisch Westfälische Technische Hochschule, Aachen, Germany, third edition, 1993.

[Ka06] M.C. Kang, *Essential dimensions of finite groups* `arxiv:math/0611673`, 2006.

[KM06] N. Karpenko, A. Merkurjev *Canonical p-dimension of algebraic groups*, Adv. Math. 205, **2** (2006), 410–433.

[KM08] N. Karpenko, A. Merkurjev *Essential dimension of finite p-groups* Inventiones mathematicae, **172** (2008), 491–508.

[KLS08] H. Kraft, R. Lötscher, G. Schwarz *Compression of Finite Group Actions and Covariant Dimension II* `arXiv:0807.2016`, 2008.

[KS07] H. Kraft, G. Schwarz *Compression of Finite Group Actions and Covariant Dimension* J. Algebra **313** (2007), 268–291.

[Le07] A. Ledet *Finite Groups of Essential Dimension One* J. Algebra **311** (2007), 31–37.

[Le04] A. Ledet *On the essential dimension of p-groups* Galois Theory and Geometry with Applications, Springer Verlag, 2004, 159-172

[MAGMA] W. Bosma, J. Cannon, C. Playoust. *The Magma algebra system. I. The user language.* J. Symbolic Comput., **24(3-4)** (1997), 235–265.

[Na47] T. Nakayama *Finite Groups with Faithful Irreducible and Directly Indecomposable Modular Representations* Proceedings of the Japan Academy **23** 1947, 22–25.

[Re04] Z. Reichstein *Compressions of group actions* Invariant Theory in all Characteristics, CRM Proc. Lecture Notes vol. **35**, Amer. Math. Soc., Providence, **35** (2004), 199-202.

[SAGE] W. Stein, *Sage: Open Source Mathematical Software (Version 3.0.6)*, The Sage Group, 2008, `http://www.sagemath.org`.

[Se64] J.P. Serre *Cohomologie Galoisienne*, lecture notes in mathematics, Springer-Verlag, 1964.

[Sh30] K. Shoda, *Über direkt zerlegbare Gruppen*, journ. Fac. Sci. Tokyo Imp. Univ. Section I, Vol. **II-3** (1930); correction, Vol. **II-7**(1931).